HMICFRS

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services

Fraud: Time to Choose

An inspection of the police response to fraud

April 2019

ISBN: 978-1-78655-784-1

www.justiceinspectorates.gov.uk/hmicfrs

Contents

Foreword

In many ways, fraud is a unique type of crime. There is more of it than there is of other crimes, it is often complex and it has no respect for jurisdictional boundaries. Victims and offenders are often remote from one another, as are the agencies that tackle fraud. Unlike other crimes, there is a national process for reporting fraud and deciding which cases will be investigated.

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) is not the first organisation to assess the law enforcement response to fraud. We recognise that a lot of changes have been made over many years to improve structures and processes, particularly at the national level. But it remains the case that, outside those organisations that have a specific national-level responsibility for fraud, it is rarely seen as a priority.

This is understandable, given the many competing priorities that police and law enforcement agencies need to cope with. Nonetheless, people are more likely to be victims of fraud than any other crime. Competing priorities only make it more important that processes are efficient, and performance must be managed to provide the best possible service that available resources will allow.

The current model of local investigations supported by national functions is the right one. And we have, as ever, found examples of some excellent work that is being done to tackle fraudsters and support their victims, particularly at a local level. But the police need a much more coordinated national approach with clear roles and responsibilities, clear operating procedures and a commitment to provide resources for the long term.

Sadly, we have found too many examples of processes that are inefficient and organisations that are not being properly held to account for their performance. As a result, many victims of fraud are not receiving the level of service they deserve.

These examples, which make sorry reading, include:

- forces being unable to provide basic data relating to the demand presented by fraud; for example, 7 of the 11 forces we inspected were unable to tell us how many of the reports of fraud that they received directly, resulted in attendance or other police activity;
- the ineffectual use of intelligence products (such as monthly victim lists) given to forces by the National Fraud Intelligence Bureau; in one force, this list was only used to count the number of victims in the force and not to identify those who needed support;

- a lack of awareness among investigators and supervisors of important resources such as authorised professional practice and the fraud investigation model; and

- some forces seeking reasons not to investigate allegations of fraud – one force filed, with no further action, 96 percent of the cases it received from the National Fraud Intelligence Bureau; some of these cases had a good degree of evidence, including identified suspects. Staff performing this role were clear that their function was to ‘reduce demand’.

In many of our reports, we would be unequivocal in our criticism, declaring these examples intolerable. And, of course, they are. However, it is not hard to fathom how these situations have come about. As we were told by one officer, “fraud does not bang, bleed, or shout”. Faced with those choices, chief constables and police and crime commissioners have difficult decisions to make.

But, although we understand why fraud may not be considered a priority for some organisations, it does not follow that we accept that the current position should be allowed to prevail. We believe that the recommendations contained within this report as well as other developments, such as the introduction of the National Economic Crime Centre, provide a real opportunity for change that should be taken.

There is a choice to be made. Leaders in government and police forces can either continue to respond to fraud in an inconsistent manner, often leaving victims confused and disillusioned, or they can act to ensure that there is a clearer strategy, less variation in service between forces and better communication with the public.

Much of this has been tried before, but it has not worked properly. Until it is made to work, with strong leadership, the chance of becoming a victim of fraud will remain too high, as will the chance of fraudsters getting away with their crimes.

It is time to choose.

Summary

The Home Secretary commissioned HMICFRS to carry out this inspection of the police response to fraud. The inspection took place between March and July 2018.

There now follows a 16-page summary of our findings followed by our recommendations and identified areas for improvement.

What we assessed

We inspected the effectiveness and efficiency of the police response to fraud, including online fraud. In doing so, we assessed whether:

- law enforcement has a well-designed strategy for tackling fraud;
- organisational structures provide the necessary capacity, capabilities and partnerships; and
- victims of fraud receive a high-quality response.

Our inspection included fraud against individuals and businesses but not fraud against those public authorities that have responsibility for dealing with fraud against their own organisations.

Our full terms of reference can be found at Annex A – Terms of reference.

Methodology

During the inspection, we visited 11 police forces in England and Wales, all nine regional organised crime units, the National Crime Agency, Action Fraud, the National Fraud Intelligence Bureau and Europol. We invited the local policing body for each of the 11 police forces to give us their views.

We spoke to people from each agency and reviewed policies and documents relating to fraud, as well as fraud case files, and we listened to calls from fraud victims. We asked forces to provide us with fraud-related data. We also engaged with an external reference group and sought advice from its members throughout the inspection.

Full details of our methodology can be found at Annex B – Methodology.

Headline findings

The law enforcement response to fraud is disjointed and ineffective

There is no national strategy for tackling fraud. Police forces have therefore developed a range of different responses. We found some examples of good practice but, taken as a whole and given the scale of fraud, not enough is being done. When it exists, good practice is not always disseminated or widely adopted.

Roles and responsibilities are not clear

Across police forces, regional organised crime units and national bodies, there is no clear understanding of who is responsible for fraud-related activities or what the expected level of performance is. Some worthwhile activities are duplicated unnecessarily; others are not carried out at all.

We found few forces that make good use of the intelligence provided by the National Fraud Intelligence Bureau or share information with it uncovered as part of investigations.

There are pockets of good prevention work

We found good examples of locally led fraud prevention work and other examples of the police and the private sector working well together. The value of this work needs to be exploited, by the police and other bodies, on a wider basis and in a more structured way.

Existing organisational structures are not working well

The principle of locally owned investigations supported by national functions is sound but its application is not. The identified national threat includes fraud, but it is often not included in the national and regional tasking processes.

We found few police forces with local strategies or clear guidance about how they intended to tackle fraud. There are unacceptably wide variations in the quality of case handling and prioritisation, unnecessary delays in the system, and fraudsters are rarely targeted proactively.

Vulnerable victims receive a good service but most victims do not

In particular, vulnerable victims generally receive good care and advice on how to protect themselves. Other victims are often given confusing and misleading advice about how (or whether) their case will be investigated and, if it is, how it is progressing.

Summary of findings

Strategy: How well designed is the strategic approach for tackling fraud?

In the absence of a government or national policing strategy for tackling fraud, we found that police forces have developed a range of different responses to fraud based on local priorities. While some represent good practice, they are far from sufficient to cope with the scale of fraud nationally.

Fraud is different. It is reported, recorded, assessed and allocated for investigation differently from other crime. While the police have an important role in investigating offences and pursuing suspects, the responsibility for protecting the public from fraud is less clear. National and local government, and the private sector (particularly the financial and telecommunications industries), all have a role to play.

We found that forces and regional organised crime units were, in the main, focused on the investigation and prosecution of fraud. There was little evidence of resources being available to disrupt or prevent fraud being committed in the first place.

City of London Police: the national lead force for fraud

City of London Police is the national lead force for fraud and responsible for Action Fraud and the National Fraud Intelligence Bureau. The force is funded by grants from the Home Office for these functions. These grants are agreed on an annual basis but we found that this inhibits long-term planning and investment. In addition, we did not find sufficient evidence of the force being effectively held to account in relation to how it carries out these functions.

Over recent years, City of London Police has produced a ‘draft’ national policing fraud strategy, a ‘draft’ national policing fraud protect strategy, and a national fraud threat and capability assessment. We found that these were not being put to practical use by the forces we inspected.

City of London Police should remain the national lead force for fraud and continue to have responsibility for the functions of Action Fraud and the National Fraud Intelligence Bureau.

The need for a national policing fraud strategy

The grant arrangements for City of London Police do not require the force to produce a national policing strategy. We believe they should. Throughout the inspection, we were told that there was a need for a national policing strategy that clearly articulates roles and responsibilities of policing at local, regional and national levels.

In 2017, the National Police Chiefs' Council (NPCC) approved a "roles and responsibilities grid for responding to private sector fraud against individuals or corporates", identifying just this. However, we found little awareness of it across policing. Those who were aware of it reiterated concerns that it was not based on a realistic understanding of capacity or capability.

The setting out of clear roles and responsibilities is sound. However, this must be done with a clear understanding of capacity and capability, and must be publicised widely to assist understanding and implementation.

Local priorities and activity

In only two of the forces we inspected was fraud made an explicit priority. Some forces included fraud within other priorities of tackling economic crime or protecting vulnerable people. Fraud was often said to not score highly enough to be considered a priority when compared with other crimes such as those relating to firearms, controlled drug supply and child sexual exploitation.

How well understood is the fraud threat?

The *National Strategic Assessment of Serious and Organised Crime 2018*, produced by the National Crime Agency, sets out the scale of threats presented by organised crime, including fraud. But the understanding of the threat from fraud is inconsistent across police forces. The National Fraud Intelligence Bureau provides 'monthly victim lists', 'six-monthly force profiles' and 'alerts'. Each of these intelligence products was used inconsistently by forces and regional organised crime units, and at times not at all. In some cases, this was due to a lack of awareness of them but we were also told that the content and timeliness of these products inhibited the effective use of them by forces. This was evident in force management statements.

A national intelligence requirement?

Most forces and regions were unaware of the eight priority areas for intelligence gathering identified by the National Fraud Intelligence Bureau. Staff in regional organised crime units stated that they had not seen the force profiles and were unaware of the demand or threat from fraud in their region. This leaves forces and regions working in isolation.

Because fraud was often not considered a priority, it did not routinely form part of local or regional intelligence-gathering requirements.

The inability of forces and regions to access fraud data held within the National Fraud Intelligence Bureau system ('Know Fraud') was often stated as an obstacle to improving the understanding of the demand from fraud.

Organised crime group mapping

Only one of the forces we inspected routinely identified and mapped organised crime groups primarily involved in fraud.

How are good practice and 'what works' highlighted?

We found little evidence of forces reviewing the effectiveness of fraud-related initiatives. We were told that there was "not a defined process" for dissemination of good practice.

The role of City of London Police in sharing best practice advice

City of London Police does undertake some activity to encourage the adoption of effective practices by forces but this task is not explicitly included within the grant agreement with the Home Office. We believe it should be a role for the lead force for fraud.

City of London Police is responsible for a number of initiatives that include peer reviews, the Economic Crime Academy, national user groups and the fraud investigation model. However, these activities fall short of a structured and methodical approach to identifying, evaluating and sharing 'what works'.

City of London Police could make more use of Police Online Knowledge Area (POLKA) provided by the College of Policing to disseminate innovation and good practice.

Structure: How well do current structures help law enforcement to tackle fraud?

We found that the scale and reach of fraud challenges the local policing model, that local and regional policing structures are inadequate, and dedicated fraud resources are, at best, limited in number. There is an inadequate understanding of the roles and responsibilities across policing for responding to fraud.

How well do police forces understand the demand from fraud?

The demand from fraud is not widely understood by police forces.

We asked the forces inspected to provide some fraud-related data. Some were unable to provide:

- the total number of frauds recorded;
- how many fraud crime reports had been allocated for investigation;

- how many reports of fraud they had received directly had resulted in attendance or other police activity; or
- the outcome of the case.

Also, in all 11 forces' data, there were discrepancies between the number of disseminations that the National Fraud Intelligence Bureau stated that they had sent to the force and the number the force had recorded.

We found that fraud was generally not prioritised and, as a result, analysis was limited. Beyond that, there are several reasons for an inadequate understanding of demand. For instance, fraud is not recorded, like other crimes, by police forces: it is recorded by the National Fraud Intelligence Bureau. Frauds for investigation are then allocated to police forces. It is these investigations that police forces are required to make a record of.

Police forces are also required to make a record of frauds reported to them that they treat as a call for service, as well as reporting them to Action Fraud so that they can be recorded by the National Fraud Intelligence Bureau.

How well do capability and capacity match identified and anticipated demand?

In the forces we inspected, the proportion of staff dedicated to fraud varied considerably with, in most cases, limited understanding why.

Some forces had small fraud investigation units of two staff while others had no dedicated fraud team. Fraud investigations were sometimes undertaken in economic crime units or financial crime teams with responsibility for all economic crime, including money laundering and asset recovery as well as fraud.

We were told that resources had been diverted away from fraud to priority crimes and we found some fraud teams with capacity to deal with just one investigation at a time. This meant that other frauds, including complex or complicated cases, were allocated to investigators who were not fraud trained. We also found that these staff had supervisors who were not fraud trained.

This lack of capacity and capability has an adverse effect on the quality of service provided to victims of fraud.

Forces allocate calls for service and National Fraud Intelligence Bureau disseminations differently. Calls for service are dealt with and allocated like most other crimes, according to local force policies. National Fraud Intelligence Bureau disseminations are received at a central point in force. In some cases, the National Fraud Intelligence Bureau decision to allocate the crime to that force is reviewed. In all cases, a decision is then made by a supervisor or 'triage' team as to whether the force will investigate the crime.

We found that in some forces all the disseminations were allocated for investigation. In one force, we found that only 10 percent of disseminations from the National Fraud Intelligence Bureau were allocated for investigation. In some of the cases not investigated, we found a good degree of evidence including identified suspects. Staff making the decisions to not investigate told us their role was to 'reduce demand'.

We understand the need to prioritise. However, some forces have set up teams to suppress demand to match capacity, rather than gaining an understanding of demand and developing capacity to meet it.

We found that regional organised crime units have different structures for dealing with fraud and there were few examples where regions had prioritised fraud. While some have dedicated fraud teams, albeit in one region this consisted of one investigator, others have merged fraud investigators and financial investigators into financial crime teams, with a greater focus on confiscation and asset recovery than on fraud. One region had no dedicated fraud investigation team and limited ability to investigate complex or serious fraud.

Some forces had more capacity and capability than their regional organised crime unit and had stopped referring fraud cases to them because of an actual or perceived lack of capacity. As a result, some regional fraud teams had reduced in size.

Action Fraud and the National Fraud Intelligence Bureau

Staffing at Action Fraud and the National Fraud Intelligence Bureau was matched to the allocated budget, but the budget had not increased with the increase in frauds reported. We saw little in terms of demand management in the contact centre and we were given data that revealed that at Action Fraud:

- average call length had risen from 12 minutes in 2012 to 19 minutes in 2018 increasing the demand on call takers;
- abandoned calls were at 37 percent for the year to March 2018; and
- between April 2016 and March 2018, call waiting times had increased from eight minutes to 16 minutes on average.

Demand on National Fraud Intelligence Bureau staff is determined by algorithms in the Know Fraud system, as well as some local searches carried out by staff. At the time of inspection, we found that there was a delay of up to three months in processing cases and the threshold for manual review of cases by staff had been raised. This meant that some of the cases identified by the Know Fraud system would not be reviewed.

National Crime Agency

Fraud and economic crime, while featured as one of nine national threats in the *National Strategic Assessment of Serious and Organised Crime 2018*, is not identified as a national priority threat. Consequently, the National Crime Agency does not have dedicated fraud teams but will allocate resources to complex frauds on a case-by-case basis.

Are the necessary partnerships in place to tackle fraud?

We found examples of the police working well with industry, local government and third sector organisations to protect the public and provide support to victims.

At the national level, there are some well-established partnerships. However, at the local level, partnerships often rely on short-term funding with no clear indication of what will happen when the funding ceases.

National partnerships

The Joint Fraud Taskforce was established in 2016 to tackle fraud at a high level: "a partnership between banks, law enforcement and government to deal with fraud and to focus on issues that have been considered too difficult for a single organisation to manage alone". It is not within the scope of our inspection.

The Banking Protocol is an example of a partnership between policing and the finance industry to provide a consistent national response to vulnerable victims of fraud.

Specialist units

Specialist units within City of London Police receive funding from private industry or government to focus on specific areas of fraud and economic crime. These include the Dedicated Card and Payment Crime Unit and the Insurance Fraud Enforcement Department.

Regional and force arrangements

We found evidence of forces and regions having developed, or developing, serious and organised crime strategic partnership groups. These generally involved local authorities, Trading Standards and voluntary organisations but fraud was not always identified by these groups as a threat.

While there was more evidence of partnership working at a local rather than a regional level, we found that most groups were established in an ad hoc way and often relied on short-term funding and motivated staff, in the absence of strategic direction.

Protect: How well do police forces help to protect individuals and businesses from fraud?

Although fraud is specifically included in the 2016 *Modern Crime Prevention Strategy*, we found very little reference to it by officers and staff. Forces relied to some extent on 'Cyber Protect' staff to provide advice to the public on how to protect themselves from computer-enabled fraud.

National campaigns

National campaigns supported by government and the financial sector are promoted by policing as a major part of fraud protect advice. Examples include 'Take Five to Stop Fraud' and 'Get Safe Online'.

The National Fraud Intelligence Bureau brings together national agencies to develop advice, campaigns and alerts to provide a consistent message that can be delivered by forces. However, we found inconsistent use of these products by forces. In some cases, investigating officers developed their own campaigns without knowing about those provided nationally.

We also found that there was little evaluation of the effectiveness of these resources and how they were used by forces.

Protect advice at first point of contact and during investigation

We found that victims were often not given fraud prevention advice when reporting fraud. During investigations, we found some occasions when investigators identified trends or risks to specific groups and worked with those groups to provide protect advice. This activity was generally reactive rather than proactive.

We were told that, when fraud protect advice was given, it was focused towards individuals rather than businesses. Officers stated that businesses were more difficult to engage with than individuals, but we found that two regional organised crime units had worked with academia to understand business needs and to assist in giving protect advice.

The provision of fraud protect advice is an essential part of preventing fraud. The ability to focus that advice towards those who are at increased risk can be effective. We found that, when advice was targeted, it was often aimed at offence types rather than categories of people.

Information provided by the National Fraud Intelligence Bureau to assist forces and regions to identify both victim and offence trends and to protect people was not always used, and at times forces were not aware of its existence.

Investigation: How well do police forces investigate fraud and deter potential offenders?

The principle of locally owned investigations supported by national functions is sound but its current application is not. At all levels, we found significant problems with the way fraud is currently investigated, including numerous examples of inefficient and ineffective processes.

There are unacceptably wide variations in the quality of case handling and prioritisation, unnecessary delays in the system and a lack of proactive targeting of fraudsters, with little evidence of forces trying to prevent or restrict them from committing further offences.

During this inspection, we did not identify any discernible difference in the way frauds reported by public sector organisations were investigated, compared with those reported by individuals or businesses.

Action Fraud and the National Fraud Intelligence Bureau both fulfil their function to varying degrees but there are problems with the current arrangements.

The centralised reporting system was set up because the 2006 *Fraud Review* identified problems with consistent recording and intelligence sharing for fraud between the 43 police forces in England and Wales. Moving away from a centralised system would recreate the problems that existed in 2006. During the inspection, no alternative was identified.

We conclude that City of London Police should retain responsibility for Action Fraud and the National Fraud Intelligence Bureau but the force should be held to account for their effectiveness and efficiency.

Telephone calls to Action Fraud are generally recorded well, and subject to audit and review by supervisors to check for accuracy and to identify best practice. However, online reports cannot be audited in the same way because they are completed by victims who may fail to provide all relevant information. There were also occasions when information was missing from online reports completed by police officers.

Within the National Fraud Intelligence Bureau, we found delays of up to three months in staff carrying out case reviews. In addition, when forces return cases to the bureau for reallocation to another force, it can take up to four weeks for a decision to be made.

How well do police respond to and prioritise allegations of fraud?

The police response to fraud is inconsistent, irrespective of the nature of the victim being an individual, business or public sector organisation. This creates unnecessary, and at times unrecognised, additional demand on forces, as well as potential inconsistency in the level of service provided to victims.

The initial response to allegations of fraud

Despite the existence of Action Fraud, some fraud victims still choose to report fraud to their local police force. The definition of a call for service enables forces to identify when they should take action themselves or advise the victim to report to Action Fraud. We found that forces often extended this definition to include additional aspects, including vulnerability and the opportunity to recover evidence.

Both examples can lead to forces starting fraud investigations in cases that would not otherwise be identified for investigation when assessed by the National Fraud Intelligence Bureau. As a result, there is a lack of consistency for victims and the potential for increased demand for forces. Clarity should be given to police forces.

We found that the withdrawn Home Office circular, 47/2004, which provided forces with priorities to be taken into consideration when deciding whether to accept a fraud case for investigation, was still being used. In one force, the fraud triage policy was based directly on the wording of this circular.

Number of investigations

Two of the forces we inspected account for 46 percent of all National Fraud Intelligence Bureau disseminations for investigation in the year to 31 December 2017. Between them, they filed 37 percent of those cases without further investigation. This means that a considerable proportion of all cases identified by the bureau as having viable lines of enquiry were filed without further investigation.

National Fraud Intelligence Bureau disseminations

We found differing views about the purpose of disseminations provided by the National Fraud Intelligence Bureau. We reviewed some and found them to be intelligence packages from which investigations could be developed. However, we found that they were not easy to read or interpret and we considered they would be difficult to use for investigators who were either, not trained to deal with fraud or who were not regularly investigating it. These documents should be easier to interpret and use.

Skills and experience of investigators

We found that those frauds dealt with by specialist fraud investigators were generally investigated well. This was not always the case with frauds investigated by non-specialist fraud investigators.

We found that some investigators were aware of the fraud investigation model but others, who did not apply the model, were consumed with protracted investigations taking several years.

Although frauds were investigated by non-specialist investigators, some forces arranged for specialist fraud investigators to give support. We also saw examples of other agencies involved in fraud investigations, enabling the use of their powers within an investigation.

We found that analytical support for fraud investigations was the exception rather than the rule and that because fraud was not generally prioritised, the availability of analytical support was adversely affected.

Referring cases upwards – the tasking process

Most frauds are allocated to police forces for investigation but many cases cross force boundaries, involve organised crime groups or require specialist capabilities involving regional or national support.

We found little engagement on fraud cases between the forces inspected and their regions, with some investigators unaware of the advice and support available to them.

We found no formal process to request City of London Police, as the national lead force for fraud, to take on an investigation. National and regional tasking processes were generally not used for fraud so that individual forces became responsible for major cases that involved cross-border or national criminality. We were told of large-scale frauds 'bouncing around' between agencies with no agency taking responsibility for them.

The National Crime Agency has an important role to play in using its tasking powers to provide an appropriate response to the most serious or harmful cases.

Disruption

There are a range of powers to disrupt criminal activity and recover or freeze assets. While some powers are new and much broader in scope than just fraud, we did not find much evidence that they were being used in fraud cases.

City of London Police has a specialist disruptions team providing support to forces. Much of its activity relies on communication service providers assisting the police, for example by closing down websites associated with online fraud. This is particularly difficult where the service provider is outside the United Kingdom.

Disruption activity is generally not reported on. We believe that fraud disruption activity should be evaluated and best practice shared across policing.

How well do police forces recognise and interact with those involved with fraud?

We were disappointed not to find evidence of individual fraudsters being profiled by forces, nor examples of preventative or ancillary orders being used to prevent fraud.

Organised crime groups

At the end of 2017, there were 842 organised crime groups mapped in the United Kingdom that were believed to be involved in fraud. We found, however, that organised crime groups whose primary offence was fraud were generally not being mapped. Investigators told us that crime groups involved in firearms and drugs offences were more likely to be identified and mapped than fraudsters. The National Fraud Intelligence Bureau force profiles, and relevant disseminations, identify to forces where organised crime groups may be active and should be considered for mapping. However, we found that some forces and regions were not aware that this information was being provided. Not mapping organised crime groups can result in inefficient practices. We were told of one case where two regions and a force investigated the same crime group, without the knowledge of the other agencies.

Management of offenders

We did not find any evidence of fraudsters being identified for integrated offender management. We found little evidence of activity taking place to prevent people becoming involved in fraud. The evidence we did see was in relation to students being targeted to become ‘money mules’ and the use of ‘suspicious activity reports’ to identify and prevent vulnerable people from being drawn into fraud.

Victims: To what extent does law enforcement consistently provide a high-quality response to victims of fraud?

Action Fraud

The 2006 *Fraud Review* stated that it was confusing for victims to know where to report fraud and recommended that a national fraud reporting centre should be established. Thirteen years later, confusion still exists. The Office for National Statistics identified in 2018 that the main reason for not reporting fraud was “a lack of awareness of Action Fraud”.

How easy is it to report fraud?

The average call abandonment rate for Action Fraud for the 12 months to March 2018 was 37 percent. This was an increase on the previous year’s figure of 34 percent. Average call waiting time in March 2018 was 16 minutes, having increased over the previous two years.

Online reports of fraud to Action Fraud can be made at any time. Between April 2017 and March 2018, 245,997 online reports of fraud were successfully made

to Action Fraud. During the same time, 195,537 online reports were started but not completed. This was an abandonment rate of 44 percent.

At the time of this inspection, Action Fraud did not publish its call and online data.

Many victims still report fraud to police forces. While we found that generally forces advised victims well about reporting their fraud, there were still examples of officers and staff having a lack of knowledge about Action Fraud and giving incorrect advice to victims.

Advice to victims

Prior to the changes to the Action Fraud website in October 2018, victims were unable to easily obtain updates on the progress of their report and they would call Action Fraud staff who were unable to provide an update. The victim would be directed to an email address where they could seek an update. This process created additional demand on Action Fraud call handlers. The new system allows victims to create an account to track their report and use an 'online update form'.

The advice provided on force websites varies considerably, and some contain incorrect information about Action Fraud and to whom fraud should be reported.

How well are vulnerable victims identified?

The identification of vulnerability is a complex issue for forces to resolve. The central reporting process for fraud and the variations in the definition of a call for service make the complexities even more pronounced. This results in an inconsistent service to vulnerable victims. In addition, in general, businesses and public sector organisations are unlikely to be considered as vulnerable, even though the effect of fraud on small businesses is often similar to that of individuals.

We found that, in most cases, staff at Action Fraud identified vulnerability and took supporting action, including referring cases to forces to support victims.

The identification of vulnerability when fraud is reported online is a different matter. Victims are asked to complete 'impact' questions on the report but, if these are not completed or a lower-level impact response is selected, then vulnerability will not be identified.

To assist with this, staff at the National Fraud Intelligence Bureau carry out system searches of all new online reports to identify 'at risk' words to try and identify hidden vulnerability.

Each force we inspected had vulnerability (for all crimes) as a priority, and consequently fraud was often prioritised in this way.

We found that forces in general identified vulnerable victims who called the police, but we found few examples where forces were analysing the 'monthly victim lists' provided by the National Fraud Intelligence Bureau. Vulnerability is not explicitly recorded on these lists, so forces must make objective judgements based solely on the amount of money involved or the age of the victim.

Identifying additional victims

Additional fraud victims are often identified during investigations. We found a mixed approach to this across the forces and regions inspected. Some investigators would report the new fraud to Action Fraud on behalf of the victim, some would ask the victim to make the report and some did neither. Without recording the new fraud, the need for support to vulnerable victims can be missed.

The City of London Police 'contact hub' has a process of sending victims questionnaires to assess evidence and vulnerability. Some forces and regions had used this approach in their own investigations.

How well are vulnerable victims supported?

The response to vulnerable victims of fraud varied across the forces we inspected. We saw examples of established victim care units, while others identified individual staff to provide support to victims or make referrals to support agencies.

Four forces are currently piloting the use of the National Economic Crime Victim Care Unit using staff based within each force and Action Fraud. Vulnerable victims of fraud are identified and provided with support. At the time of our inspection, however, there were delays of up to three months in contacting some victims.

Operation Signature is used to different degrees in a number of forces. Its purpose is to identify and provide support to the most vulnerable victims of fraud, often based on the age of the victim.

Both victim care units and Operation Signature have been recognised as 'best practice models' by the National Police Chiefs' Council, but neither have been evaluated. Some forces inspected stated that they did not have enough resources to provide such services. We believe that an independent evaluation of these services would assist police forces and local policing bodies to determine whether resourcing them is appropriate.

The use of such approaches may reduce demand on policing by reducing repeat victimisation, but it does place additional demand on support services, many of which are third sector organisations. Staff in these support agencies told us that increasing the number of people who need support affects their ability to provide a good service when their funding arrangements are limited or short term.

How well is fraud victim satisfaction assessed and managed?

We found little evidence of forces seeking victim satisfaction information in relation to fraud. Those forces that still carried out customer satisfaction surveys did not include fraud questions. Forces have little understanding of the level of satisfaction with the service they provide to fraud victims.

Similarly, we found little evidence of Action Fraud seeking customer satisfaction feedback. Victims can complete a short survey about their online experience but we saw no activity in response to this. There was nothing to help the contact centre managers understand whether callers were happy with their service.

How well are fraud victims kept informed about progress of their reports?

Delays within the reporting and dissemination process at the National Fraud Intelligence Bureau and then within forces mean that victims can wait months before being told what will happen with their case. This is compounded when the bureau notifies the victim that their case has been sent to a force for investigation, only for the victim to receive a letter from the force saying they will not investigate it.

Maintaining contact with victims can be time consuming for investigators, especially when there are numerous victims in an investigation. Some forces and regions have identified innovative ways of keeping multiple fraud victims updated, for example by using volunteers and dedicated victim care staff and using pre-agreed passwords to reassure victims of the genuine nature of the call. However, we found one specialist fraud team that had no method for managing contact with victims.

There are many reasons why fraud may not be investigated, including availability of resources or prioritisation. Often fraud suspects may be outside the legal jurisdiction of the United Kingdom and no arrangements with the other country to progress the investigation, albeit we found examples of cases where those arrangements existed but no investigation took place. Victims should still be told of the decision to not investigate and have the rationale explained to them.

We found one force that, having made the decision not to investigate a fraud allegation, routinely notified victims of this but did not explain why. Forces should be providing an explanation to victims for their decisions in these cases.

Recommendations

We have made 16 recommendations in this report. For ease of reference, we have drawn them together in a single chapter here and organised them by reference to those to whom they are addressed.

To the NPCC Coordinator for Economic Crime

Recommendation 1

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should publish a timetable for implementing the revised Know Fraud system, making clear which services are to become available at each stage of implementation and thereby enabling forces to make use of each service as early as practicable. The use made of the system by police forces should be monitored and evaluated to identify best practice.

Recommendation 5

The National Police Chiefs' Council (NPCC) Coordinator for Economic Crime, in consultation with the Home Office and the Director General of the National Economic Crime Centre, should develop a national policing strategy for fraud and, by 31 March 2020, secure its approval by the NPCC for adoption by all police forces. The strategy should:

- make clear the roles and responsibilities of police forces and regional organised crime units;
- define the relationship between City of London Police as the national lead force, the National Crime Agency (in particular the National Economic Crime Centre) and other relevant bodies, seeking to ensure that their respective roles and responsibilities complement each other and avoid duplication; and
- define how fraud intelligence will be developed, disseminated and put to effective use by police forces and the National Fraud Intelligence Bureau.

The implementation arrangements for the strategy should include clear communication and review processes.

Recommendation 7

By 31 March 2020, the National Police Chiefs' Council Coordinator for Economic Crime should carry out an evaluation of two National Fraud Intelligence Bureau products: monthly victim lists and six-monthly force profiles. The evaluation should include:

- consulting with police forces to establish the uses to which these intelligence products are put; and
- identifying any opportunities to improve the products' utility or reduce the burden on the National Fraud Intelligence Bureau in compiling them.

Recommendation 8

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should issue guidance to police forces on how to:

- accurately record and report on National Fraud Intelligence Bureau 'disseminations for enforcement' to ensure consistency and clarity for fraud-recording processes (the guidance should reassert the requirement in the Home Office Counting Rules for forces to provide the case number, the crime numbers, the suspect details and the outcome details for each such dissemination);
- determine their response to National Fraud Intelligence Bureau disseminations for enforcement, ensuring consistency and clarity for victims of fraud; and
- ensure that, when a force decides not to investigate, or not to continue an investigation, the victim is provided with a clear written explanation of the rationale for that decision.

Recommendation 10

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime, when issuing to police forces advice on fraud protection that is to be given to the public (including alerts and campaigns), should take responsibility for evaluating the effectiveness of how that advice is given to the public and the effectiveness of the advice.

Recommendation 11

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should issue guidance to police forces in relation to fraud-related calls for service as described in the Home Office Counting Rules. The advice should make clear to forces the circumstances in which they are expected to intervene and the circumstances in which they may refer the case direct to Action Fraud.
The advice should also make clear how:

- responses to reports of fraud may adequately meet the needs of victims;
- vulnerable victims should be identified and dealt with appropriately; and
- reports of fraud should be efficiently referred to Action Fraud.

Recommendation 12

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should redesign the National Fraud Intelligence Bureau dissemination for enforcement documentation to make it easier for recipients to interpret and use.

Recommendation 14

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime should:

- carry out (and subsequently evaluate) a campaign to raise the public awareness of the existence and role of Action Fraud; and
- provide chief constables with a description of the role of Action Fraud for uploading to force websites.

Recommendation 15

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime should take steps to remedy the absence of published performance indicators at Action Fraud. As soon as practicable, performance indicators should be set in relation to, for example, call handling waiting times and abandonment rates, online reporting and victim satisfaction levels. Thereafter, information on performance against those indicators should be published.

Recommendation 16

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should provide guidance to Action Fraud and chief constables. This is to ensure that, promptly on reporting a fraud, victims are provided with explanations of:

- the role of Action Fraud;
- the process by which their fraud report will be considered for assessment or referral to the police (or other law enforcement agency) by the National Fraud Intelligence Bureau;
- how to obtain an update on the progress of their case;
- how, following referral from the National Fraud Intelligence Bureau, the decision on whether and how to investigate rests with the police (or other law enforcement agency); and
- the options open to victims of fraud to seek civil redress as an alternative (in cases where criminal investigations are not carried out or do not lead to convictions).

To the NPCC Coordinator for Economic Crime and chief constables

Recommendation 2

By 31 March 2020, the National Police Chiefs' Council Coordinator for Economic Crime and chief constables should ensure that forces have processes in place to accurately and efficiently report fraud outcomes to the National Fraud Intelligence Bureau.

To chief constables

Recommendation 9

By 30 September 2019, chief constables should publish their force's policy for responding to and investigating allegations of fraud (in relation to both calls for service and National Fraud Intelligence Bureau disseminations for enforcement).

To the Home Office

Recommendation 4

By 30 September 2019, the Home Office should publish information concerning its agreement with City of London Police to act as the national lead force for fraud. The published information should include (as a minimum) descriptions of:

- the aims and objectives of the agreement;
- the funding arrangement;
- accountability and governance processes; and
- City of London Police's performance against the agreement.

To the NPCC Coordinator for Economic Crime and the College of Policing

Recommendation 6

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime, working with the College of Policing, should take responsibility for identifying, evaluating and disseminating best practice advice on the police response to fraud.

To the Director General of the National Crime Agency and the NPCC Coordinator for Economic Crime

Recommendation 13

With immediate effect, the Director General of the National Crime Agency, in consultation with the National Police Chiefs' Council Coordinator for Economic Crime, should ensure that the tasking powers of the National Crime Agency are used effectively in the case of serious and organised fraud.

To the Economic Crime Strategic Board

Recommendation 3

By 31 August 2019, the Economic Crime Strategic Board should extend its remit to include all forms of fraud against individuals and businesses, not just serious and organised fraud.

Areas for improvement

There are some areas in which we think chief constables need to make improvements but we have not made specific recommendations about how they should do this. Chief constables should:

1. improve the way their force uses the National Fraud Intelligence Bureau monthly victim lists to identify and support vulnerable victims and others who require additional support;

2. ensure their forces improve the identification and mapping of organised crime groups in which the principal criminality is fraud;

3. ensure that fraudsters are included among those considered for serious organised crime ‘prevent’ tactics, including by local strategic partnership boards and through integrated offender management processes;

4. increase their force’s use of ancillary orders against fraudsters; and

5. ensure that their force complies with the Code of Practice for Victims of Crime when investigating fraud.

1. Introduction

About our inspection

1.1. This report details the findings of an inspection commissioned by the Home Secretary.

1.2. We inspected the effectiveness and efficiency of the law enforcement response to fraud, including online fraud. This included fraud against individuals and businesses but not fraud against those public authorities that have responsibility for dealing with fraud against their own organisations.

About fraud

1.3. Fraud takes many forms but offences of fraud are generally deceptions committed to make a financial gain.

1.4. While fraud is normally a financially motivated crime, not all financial crimes are fraud. The manufacture and use of counterfeit currency, money laundering offences and corruption crimes are not included in our inspection. Information about legislation and the types of fraud can be found at Annex C – Legislation and types of fraud.

The scale of fraud

1.5. According to the Crime Survey for England and Wales, in the last four years, fraud made up almost one-third of the total crime and was the largest stand-alone crime type.[1]

1.6. Adults are more likely to be a victim of fraud than any other crime type.[2]

1.7. However, many instances of fraud are not reported. In the year ending June 2018, the Crime Survey estimated that there were 3.3 million incidents of fraud (accounting for almost a third of all crime) while only 0.6 million were reported to the National Fraud Intelligence Bureau.[3] The Office for National Statistics reported over 641,700 fraud crimes recorded in the year July

[1] Crime in England and Wales: Appendix tables, Office for National Statistics, 2019

[2] Crime in England and Wales: Year ending June 2018, Office for National Statistics, 2018

[3] *Op cit*, Little change in the volume of fraud offences in the last year

2017 to June 2018, which puts recorded fraud at about 11 percent of all recorded crime.[4]

The harm from fraud

1.8. Some victims report losing their entire lifetime's savings through fraud. For others, relatively small losses can have an equally devastating impact.

1.9. It is not just financial loss that creates harm. The psychological and emotional damage caused by fraud can be enormous.

1.10. The harm from fraud is not just limited to the direct harm caused by each offence. The proceeds from fraud can be used to fund serious organised crime and, in some cases, terrorism. In 2017, the UK Fraud Costs Measurement Committee estimated the total cost of fraud to the United Kingdom economy to be £190 billion[5] – which is nearly 10 percent of gross domestic product.

1.11. There should be no doubt that combating fraud, and those who commit it, is important.

The police response to fraud

1.12. In England and Wales, fraud is reported through a central reporting process and cases are allocated to police forces for investigation. They are allocated on the basis of viable lines of enquiry rather than the location of the offence.

1.13. All reports of fraud should be received by Action Fraud, even if the victim contacts the police in the first instance. The National Fraud Intelligence Bureau then allocates cases to police forces for investigation. It also produces intelligence about fraud. Action Fraud and the National Fraud Intelligence Bureau are both run by City of London Police.

1.14. Depending on the nature of the case, fraud investigations may be carried out by a local force, a regional organised crime unit or the National Crime Agency.

1.15. All these organisations contribute to, or directly provide, advice to individuals and businesses about how to protect themselves from fraud.

---

[4] Based on Office for National Statistics data set for the year ending June 2018, this includes public reports to Action Fraud as well as industry reports to Cifas and UK Payments from member parties. Computer misuse offences have been removed for the purpose of this report. The full table of statistics is available. This is still considered experimental data by the Office for National Statistics.

[5] *Annual Fraud Indicator 2017: Identifying the cost of fraud to the UK economy*, UK Fraud Costs Measurement Committee, 2017

Context

Recent changes to the fraud landscape

1.16. Concerns about how fraud is dealt with are not new.

1.17. In 2005, the then Attorney General commissioned a review of the arrangements for dealing with fraud across the whole of the criminal justice system in England and Wales. The objective was to reduce the instances of fraud and the damage that they cause to the economy and society.

1.18. The 2006 *Fraud Review* identified many problems with how fraud was reported to and recorded by the police; the absence of coordinated fraud prevention activity; and the lack of fraud investigation and intelligence-gathering capability within police forces.

1.19. The review made a total of 62 recommendations (on pages 310–321) ranging across government, policing and the wider criminal justice system. This resulted in structures being created that were intended to provide a more coordinated and nationally consistent approach to fraud:

- In 2006, City of London Police became the national lead force for fraud, with responsibility for the National Fraud Intelligence Bureau, and the Home Office created the National Fraud Reporting Centre.
- In 2008, the National Fraud Strategic Authority, later to become the National Fraud Authority, was established. Its purpose was to set the strategy for the national response to fraud. In 2009, it published *The National Fraud Strategy: A new approach to combating fraud*.
- In 2009, the National Fraud Reporting Centre was renamed 'Action Fraud'.
- In 2013, the National Fraud Authority published *Fighting Fraud Together: The strategic plan to reduce fraud*. This document was endorsed by 37 co-signatories from a range of public and private sector bodies.
- In 2014, the National Fraud Authority was closed and its responsibilities shared across government agencies. Responsibility for setting the national response to fraud transferred to the newly established National Crime Agency and responsibility for Action Fraud transferred to City of London Police. Following this, the notion of a single national fraud strategy such as *Fighting Fraud Together* was largely forgotten.
- In 2015, City of London Police circulated a draft *National Policing Fraud Strategy*. This document was intended to provide guidance and support to police forces. However, we did not find any evidence of general

awareness of the document, or that it had ever been formally adopted by police forces.

1.20. The net result of all these changes is that there is no current government or national policing strategy for tackling fraud.

Action Fraud and the National Fraud Intelligence Bureau

1.21. Action Fraud remains the single reporting centre for all fraud and cyber-crime reports from members of the public. It receives crime reports and information reports in one of four ways:

- Directly from members of the public over the telephone (8am–8pm Monday to Friday for fraud).
- Directly from members of the public via the online reporting tool on the Action Fraud website.
- Directly from police forces or other law enforcement agencies on behalf of victims through the online reporting tool on the Action Fraud website.
- Directly from businesses using the online bulk reporting tool on the Action Fraud website.

1.22. The National Fraud Intelligence Bureau processes the information received by Action Fraud, along with information supplied by other agencies such as Cifas[6] and UK Finance[7], on the Know Fraud system. When an investigation appears viable, it is allocated to a police force or other law enforcement agency for investigation. The bureau also provides forces and agencies with intelligence products. These include:

- **Victim care packages** – these relate to particularly vulnerable individuals, who have reported a crime or information, and are sent to the victim's local force to provide additional support.
- **Monthly victim lists** – these contain the details of all the victims reporting to Action Fraud residing in each specific police force (based on the address provided by the victim in the report). A monthly schedule of this information is forwarded to every police force and includes crime type, the victim's details and the impact of the offence on the victim.

[6] Cifas is a not-for-profit organisation working to reduce and prevent fraud and financial crime in the UK.

[7] UK Finance is the trade association for the finance and banking industry operating in the UK.

- **Six-monthly force profiles** – these are produced biannually and provide statistical analysis of crime trends, crime types and emerging crime techniques used by offenders within that force area and nationally.

- **Threat updates** – these support a national profiling of current and emerging fraud, and the prevention advice to the public that sits alongside this profiling.

1.23. Neither Action Fraud nor the National Fraud Intelligence Bureau is responsible for the investigation of offences. That duty remains with the local police force or other appropriate law enforcement agency.

Know Fraud database

1.24. Know Fraud is the National Fraud Intelligence Bureau's intelligence system. The system identifies links and patterns in offending, electronically assessing all reports for solvability factors.[8]

1.25. Unlike other crimes for which police forces hold their own intelligence and information on their own systems, all fraud-related crime reports are retained by the bureau on the Know Fraud system. As a result, at the time of our inspection, individual law enforcement agencies did not have direct access to this system. This was also the case for staff within Action Fraud.

1.26. Those cases with identified solvability factors are allocated to staff within the bureau to review, analyse and develop. When there are viable lines of enquiry to pursue the offender, the matter is referred to the relevant police force or other law enforcement agency to pursue. This may not necessarily be the force area where the crime was committed or where the victim lives.

1.27. Depending on the result of the analysis, victims of crime reports[9] will receive a follow-up letter with one of two conclusions: either that no further action will be taken at that time and that the victim's details will remain on the database, or that lines of enquiry have been identified and that the case has been forwarded to a specific police force or law enforcement agency for further action.

[8] Solvability factors include information such as bank account details, names, addresses and email accounts.

[9] Persons making information reports will not receive a further update.

Changes to the reporting process and Know Fraud

1.28. Since 2014 when City of London Police took responsibility for both Action Fraud and the National Fraud Intelligence Bureau, the force has recognised that the technology that supported both Action Fraud and Know Fraud has not been fit for purpose. As a result, a project to design and implement a new system for both reporting and analysis of reports has been under way.

1.29. We do not underestimate the contractual and technical complexities that City of London Police has faced in updating the respective systems. However, it is the case that, although welcomed, these developments are significantly overdue. Planned for April 2016, the implementation was delayed by over two years.

1.30. In October 2018, initial improvements to the reporting process were introduced. However, each of the planned updates are incremental in nature with different functions being available at different times.

1.31. These changes came into effect after the completion of the fieldwork on which this report relies and, consequently, we are unable to provide comment on the effectiveness of these changes and whether they have had a positive impact on the problems we highlight in this report and, ultimately, the experience of service users.

1.32. At the time of publication of this report, the changes to Know Fraud included the following:

- A new design for the Action Fraud website.
- A revised online reporting function encouraging completion of all fields and identifying the limitations of investigation if fields are left blank.
- Asking victims to provide information that assesses both the impact the incident has had on them and their vulnerability to becoming a victim of fraud in future.
- Enabling victims to create an account with Action Fraud (either when reporting online or through the contact centre) that provides them with some ability to track the progress of their crime and receive prevention advice relevant to the fraud they reported.
- Giving victims the opportunity to request an update on their report through an online form on the Action Fraud website.
- ‘Live’ transfer of information between Action Fraud and the National Fraud Intelligence Bureau.

1.33. However, we do not know the proposed timeline for implementation of the proposed further improvements. These include the ability of police forces to directly access the system to obtain data that relate to their communities.

Recommendation 1

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should publish a timetable for implementing the revised Know Fraud system, making clear which services are to become available at each stage of implementation and thereby enabling forces to make use of each service as early as practicable. The use made of the system by police forces should be monitored and evaluated to identify best practice.

Outcomes

1.34. The National Fraud Intelligence Bureau is responsible for recording the outcomes of reported frauds. To do this, the bureau relies on police forces reporting the outcomes of the disseminations for enforcement[10] they receive. Not all forces provide outcome data on a regular basis. The bureau says that the situation is getting better and they have notified those forces that need to improve.

1.35. The data that forces provide to the National Fraud Intelligence Bureau are consistent with the requirements of the Home Office Counting Rules for fraud.[11] Although the information contains a range of outcomes for crimes, it does not include disruption activity. The data therefore only provide a partial picture of the response to fraud.

1.36. That said, the data available to the National Fraud Intelligence Bureau show that only about 4 percent of reported frauds receive a criminal justice outcome.[12]

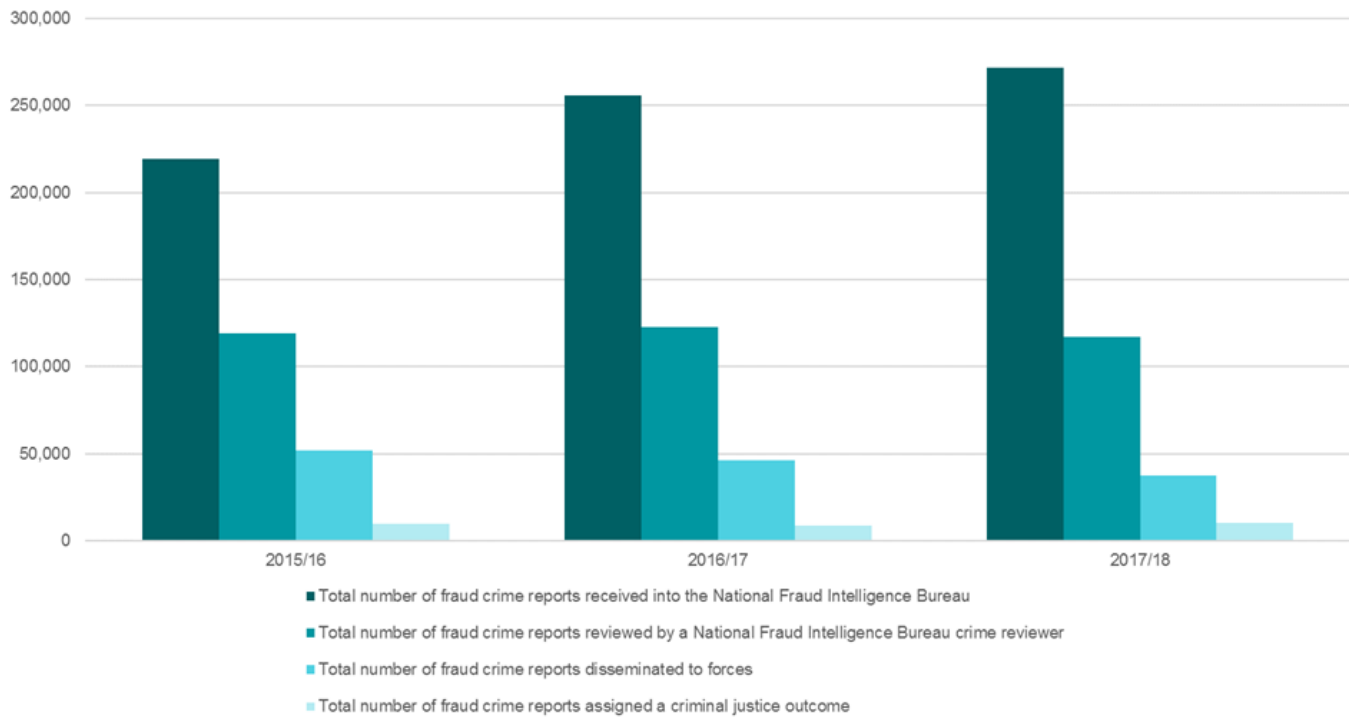
[10] Disseminations for enforcement consist of crime reports, intelligence and information identified by National Fraud Intelligence Bureau crime reviewers as having viable lines of enquiry and then allocated to police forces for investigation.

[11] A range of outcomes are required to be recorded to understand the activity that law enforcement agencies take to deal with recorded crime.

[12] Criminal justice outcomes include where the suspect is charged, summonsed or receives a formal out-of-court outcome i.e., a caution.

1.37. Despite the number of reported frauds increasing over the last three years, the number of cases disseminated to forces for investigation has reduced while the number receiving a criminal justice outcome has remained relatively static. Figure 1 shows the number of frauds reported over recent years and those allocated a criminal justice outcome.

Figure 1: Number of crime reports received, reviewed by a National Fraud Intelligence Bureau reviewer, disseminated to forces and assigned a criminal justice outcome in England and Wales in 2017/18



Source: HMICFRS data collection

Recommendation 2

By 31 March 2020, the National Police Chiefs' Council Coordinator for Economic Crime and chief constables should ensure that forces have processes in place to accurately and efficiently report fraud outcomes to the National Fraud Intelligence Bureau.

Europol

1.38. The European Union Agency for Law Enforcement Cooperation, better known as 'Europol', is the European Union's law enforcement agency. Based in The Hague, Netherlands, Europol uses analysis to support the law enforcement agencies of European Union member states to combat serious and organised crime, including fraud.

1.39. Europol use the information-sharing platform known as the ‘secure information exchange network application’ or ‘SIENA’ for sharing information between member states. SIENA is available to all United Kingdom law enforcement agencies to use (although access is provided through regional organised crime units). In addition, Europol also facilitates joint investigations and collaboration between agencies. Given that organised fraud often involves an international element, we were disappointed to find that the services provided by Europol were not widely recognised and were rarely used by the forces and regional organised crime units that we inspected.

1.40. At the time of our inspection, a regional organised crime unit officer was embedded within Europol. The post-holder assisted with regional organised crime unit and individual force access to pan-European intelligence, including fraud. Funding for this post ceased in September 2018 and was replaced by a member of staff from the National Crime Agency. Staff from the agency told us that they feared that this would result in a loss of the understanding of local policing requirements within Europol.

1.41. City of London Police has identified that it intends to provide a member of staff at Europol to facilitate an improved economic crime intelligence-sharing and development resource internationally.

2. Strategy: How well designed is the strategic approach for tackling fraud?

2.1. For this aspect of the inspection, we examined whether national and local strategies were based on a comprehensive understanding of the fraud threat. We also examined whether those strategies enabled the identification and spread of good practice.

The national strategic approach to tackling fraud

2.2. In the absence of a government strategy and a national policing strategy for tackling fraud, police forces have developed a range of different responses, based on local priorities. Some represent good practice but collectively they are far from sufficient to cope with the scale of fraud nationally.

2.3. The lack of a government or national policing strategy for tackling fraud has profound implications. These include the understanding of roles and responsibilities for responding to fraud, how the public is protected from fraud and how victims of fraud are treated by police forces.

2.4. Fraud is referred to within certain current crime-related strategies, for example, those relating to modern crime prevention[13] or serious and organised crime.[14] Some fraud is serious and organised but a large proportion of it is not. Therefore, it is not addressed by the serious and organised crime strategy. Also, in both cases, fraud is considered alongside other crime types. Consequently, the many different elements that make up the fraud threat and the possible responses to them are not dealt with in detail.

2.5. During this inspection, we were often reminded that fraud is different from other crimes, which it is. Fraud takes many forms, transcending geographical boundaries and jurisdictions. It adversely affects individuals, businesses – large and small – and public sector organisations.

2.6. As a result, the police response to fraud is also different. No other crime type (except for cyber-dependent crime) is reported, recorded and disseminated through a central reporting process. No other crime type is allocated to a force

[13] *Modern Crime Prevention Strategy*, Home Office, 2016

[14] *Serious and Organised Crime Strategy*, HM Government, 2018

for investigation based on viable lines of enquiry,[15] as opposed to the geographic location of the offence.

2.7. The Home Office recognised the exceptional characteristics of fraud as recently as July 2018 in its publication, *The scale and nature of fraud: A review of the evidence*, in which it stated: "Fraud is in many ways, a unique crime type. It overlaps with many other crime types and there is no one body or organisation that can deal with fraud in its entirety."

2.8. The role of policing in combating fraud is clearly an important one. But there is a limit to that role. The responsibility to investigate offences and pursue offenders rests, in most cases, with the police. However, the extent of the police's responsibility, for example to protect the public from fraud, is less clear. National and local government, the financial and retail sectors, telecommunication companies and many other bodies all have a role to play. In the absence of a national fraud strategy, there is no consistent and effective joint working and information sharing across all these bodies. There is an opportunity to remedy this.

2.9. In January 2019, the Government established the Economic Crime Strategic Board, jointly chaired by the Home Secretary and the Chancellor of the Exchequer, to bring together leaders from across government and the financial sector. The board's remit, in relation to fraud, money laundering and other forms of economic crime is to "set priorities, direct resources and scrutinise performance against the economic crime threat, which is set out in the Serious and Organised Crime (SOC) Strategy".[16] We believe that the board's remit should be extended.

Recommendation 3

By 31 August 2019, the Economic Crime Strategic Board should extend its remit to include all forms of fraud against individuals and businesses, not just serious and organised fraud.

[15] Viable lines of enquiry may identify information where police can take action towards an investigation.

[16] New taskforce to tackle economic crime, HM Government, 2019

Prevent, Pursue, Protect and Prepare

2.10. Government strategies for countering terrorism[17] and combating serious and organised crime[18] both use a format known as 'the 4Ps':

- **Prevent** – people from becoming involved in or supporting criminal activity;
- **Pursue** – prosecute and disrupt those engaged in criminality;
- **Protect** – individuals and businesses from criminality; and
- **Prepare** – the public and businesses to reduce the impact of criminality.

2.11. The 2015 City of London Police draft strategy also used this terminology. We have done the same in this report for ease of understanding and consistency.

2.12. A constant message from those with whom we spoke was *"*the police will not investigate [pursue] their way out of this*"*. We agree.

2.13. It was therefore disappointing to find that, with a few notable exceptions, police efforts are focused on the investigation and prosecution element of 'pursue'. For example, there was little evidence of resources being available to disrupt organised crime groups involved in fraud – wherever they were located – to stop offences being committed in the first place.

City of London Police: the national lead force for fraud

2.14. City of London Police is the national lead force for fraud and is responsible for Action Fraud and the National Fraud Intelligence Bureau. The Commissioner of City of London Police is the National Police Chiefs' Council (NPCC) lead for economic crime. The Commissioner is supported by the NPCC Coordinator for Economic Crime[19]: an officer of the rank of commander within City of London Police.

---

[17] Counter-terrorism strategy (CONTEST). The aim of CONTEST is to reduce the risk to the UK and its interests overseas from terrorism.

[18] The *Serious and Organised Crime Strategy* states at paragraph 16, "We define serious and organised crime as individuals planning, coordinating and committing serious offences, whether individually, in groups and/or as part of transnational networks. The main categories of serious offences covered by the term are: child sexual exploitation and abuse; illegal drugs; illegal firearms; fraud; money laundering and other economic crime; bribery and corruption; organised immigration crime; modern slavery and human trafficking; and cybercrime."

[19] The title 'NPCC Coordinator for Economic Crime' has previously been used interchangeably by City of London Police with the title 'National Coordinator for Economic Crime'. When the latter title has been included in the title of documents referenced within this report, we have adopted it.

2.15. To fund this activity, the force receives two separate annual grants[20] from the Home Office.

2.16. The annual nature of the grants inhibits long-term planning and investment. Senior leaders within the force told us this causes particular problems with recruitment and retention of staff, it being harder when posts cannot be guaranteed for more than 12 months. As a result, the force conducts almost continual recruitment campaigns.

2.17. Fraud is not a short-term problem. If the Home Office's intention is for City of London Police to perform the national lead force role for more than a year, a longer-term funding arrangement would be preferable. Short-term funding arrangements are a problem in other aspects of policing too, for which we have made recommendations before.[21]

2.18. The agreements relating to each grant set out arrangements by which the Home Office should monitor the force. However, we did not find sufficient evidence to satisfy ourselves that the force was being effectively held to account in relation to how it carries out these functions.

2.19. Unlike the National Crime Agency, City of London Police does not have any powers to require forces to take action.[22] Priorities for each of the 43 police forces are set by individual chief constables and police and crime commissioners. Nonetheless, City of London Police has produced several documents including a draft national policing fraud strategy,[23] a draft national policing fraud "protect" strategy[24] and a national fraud threat and capability assessment.[25]

2.20. All these documents are, in our view, worthwhile but they are not being put to good, practical use by the police forces we inspected.

---

[20] The annual funding agreement between the Home Office and City of London Corporation to deliver the services of the National Lead Force for Fraud Function 2016/17.

[21] *Regional Organised Crime Units: A review of capability and effectiveness*, HMIC, 2015, page 25

[22] The National Crime Agency has statutory powers under the Crime and Courts Act 2013 to direct chief constables in England and Wales to take action.

[23] *National Policing Fraud Strategy: Draft prepared by the National Coordinator for Economic Crime*, City of London Police, 2015.

[24] *National Policing Fraud "Protect" Strategy: Draft prepared by the National Coordinator for Economic Crime*, City of London Police, 2015.

[25] *Force Fraud Threat and Capability Assessment*, City of London Police, 2017. This document describes the calculation of the scale and impact of the fraud threat for the force boundaries in England and Wales excluding London.

2.21. We support the idea of a national lead force. Given the complex nature of fraud, it is also appropriate to have a single body responsible for the accurate recording, analysis and dissemination of intelligence to the police and law enforcement agencies. In the absence of any obvious alternatives, City of London Police is a suitable police force to hold the responsibility.

Recommendation 4

By 30 September 2019, the Home Office should publish information concerning its agreement with City of London Police to act as the national lead force for fraud. The published information should include (as a minimum) descriptions of:

- the aims and objectives of the agreement;
- the funding arrangement;
- accountability and governance processes; and
- City of London Police's performance against the agreement.

The National Economic Crime Centre

2.22. On 31 October 2018, after we had conducted the fieldwork for this inspection, the National Crime Agency launched the National Economic Crime Centre. This multi-agency centre is expected to improve the understanding of the serious and organised economic crime threat, and plan and co-ordinate the response to the most harmful cases.

2.23. It is critical that roles and responsibilities are made clear as the centre develops. We were pleased to see early engagement between the National Crime Agency and City of London Police.

The need for a national policing strategy

2.24. As we have set out earlier, the lack of a national fraud strategy that extends across the public, private and voluntary sectors, as well as government, creates a fragmented cross-sector approach to fraud.

2.25. The *Fraud Review* concluded that the national response to fraud, including that from police forces, was un-coordinated. Now, 13 years on, the police response to fraud remains too disjointed and too ineffective.

2.26. This has not gone unrecognised and City of London Police has attempted to remedy the situation (the 2015 draft strategy is one example). However, the current arrangement between the Home Office and City of London Police does not require them, as the lead force, to develop a national policing strategy for fraud. We believe it should.

2.27. Throughout the inspection, we were told there was a need for a national policing strategy that clearly articulates the roles and responsibilities of forces, regional organised crime units, City of London Police and the National Crime Agency.

2.28. This has been attempted before. As recently as January 2017, a roles and responsibilities grid[26] was presented to, and approved by, the Chief Constables Council.[27]

2.29. Created by the National Fraud Intelligence Bureau, the grid sets out expected responses at force, regional and national levels to "private sector fraud against or committed by individuals or corporates". It does this under four headings:

- Response to reported fraud.
- Pursuing United Kingdom associated individuals and groups.
- Pursuing international individuals and groups.
- Protecting and preventing fraud.

2.30. Prior to being approved by the Council, forces were consulted. We understand that several forces raised concerns with the contents of the grid. These concerns included the lack of capacity and capability at the regional level to fulfil the grid's requirements, and a lack of detail on a potential 'tasking' process.

2.31. During our fieldwork, we found little awareness of the grid among officers and staff (including those in senior positions). Furthermore, those who were aware reiterated the earlier concerns that the grid was not based on a realistic understanding of capacity or capability.

2.32. For example, within regional organised crime units, we found fraud units that had just two officers in them. Fraud investigators were invariably committed to long-term, complex investigations with little capacity for additional work. This is in stark contrast with the roles set out in the roles and responsibilities grid, which include:

---

[26] *City of London – National Coordinator for Economic Crime: Annual Review 2016/17* states at page 4: "An important first step in formalising coordination of national law enforcement activity was agreement of a grid setting out roles and responsibilities of the National Crime Agency, Serious Fraud Office, City of London Police, regional organised crime units and local police forces. This was agreed on behalf of policing by the National Police Chiefs' Council on 25 January 2017."

[27] The Chief Constables' Council is the senior operational decision-making body for the National Police Chiefs' Council. It brings together chief constables of police forces in the United Kingdom.

- “**Response to reported fraud**
    - lead complex UK cases including multi-force liaison;
    - deconflict force activity and resource allocation; and
    - provide appropriate, specialist victim response
- **Pursuing United Kingdom associated individuals and groups**
    - lead complex UK cases including multi-force liaison;
    - deconflict force activity and resource allocation; and
    - provide appropriate, specialist victim response.
- **Pursuing international individuals and groups**
    - deliver regional campaigns against UK nexus of international OCGs.
- **Protecting and preventing fraud**
    - deliver regional PROTECT and PREVENT campaigns, often with force-level assistance.”

2.33. The principle of setting out clear roles and responsibilities at local, regional and national levels is sound. However, it must be done with a clear understanding of the capacity and capability of those who will be called on to meet them. Once those roles and responsibilities have been agreed, they should be publicised widely to assist understanding, and adequate measures should be taken to secure implementation. Currently, these things have not been done.

Recommendation 5

The National Police Chiefs' Council (NPCC) Coordinator for Economic Crime, in consultation with the Home Office and the Director General of the National Economic Crime Centre, should develop a national policing strategy for fraud and, by 31 March 2020, secure its approval by the NPCC for adoption by all police forces. The strategy should:

- make clear the roles and responsibilities of police forces and regional organised crime units;
- define the relationship between City of London Police as the national lead force, the National Crime Agency (in particular the National Economic Crime Centre) and other relevant bodies, seeking to ensure that their respective roles and responsibilities complement each other and avoid duplication; and
- define how fraud intelligence will be developed, disseminated and put to effective use by police forces and the National Fraud Intelligence Bureau.

The implementation arrangements for the strategy should include clear communication and review processes.

Local priorities and activity

2.34. The National Audit Office, in its report *Online Fraud*, found that "only 27 out of 41 police and crime commissioners referred to online fraud in their police and crime plans as at April".[28]

2.35. Of the 11 forces we inspected, 2 had made fraud an explicit priority (although some did include fraud within the scope of other priorities for tackling economic crime or protecting vulnerable people). We were told that, when risk-assessed against other crime types, fraud did not usually score highly enough to be included as a priority. Matters such as firearms, controlled drug supply and child sexual exploitation were more likely to be priorities.

2.36. It was therefore not surprising that this translated into an inconsistent local approach to fraud. We found that few of the forces we inspected had local strategies or clear guidance on how they intended to tackle fraud across the full spectrum of prevent, pursue, protect and prepare.

[28] *Online fraud*, National Audit Office, 2017, paragraph 2.8

How well understood is the fraud threat?

2.37. Understanding the scale and nature of the threat presented by fraud enables resources to be deployed appropriately. It also assists in the identification of appropriate strategies and tactics to respond effectively.

2.38. Various assessments and intelligence products assist in this process.

2.39. The *National Strategic Assessment of Serious and Organised Crime 2018*, produced by the National Crime Agency, sets out the scale of threats presented by organised crime, including fraud.

2.40. The National Fraud Intelligence Bureau provides police forces with intelligence products relating to victim care: monthly victim lists, six-monthly force profiles and monthly alerts.

2.41. Despite the provision of this intelligence, at force and regional level we found an inconsistent understanding of the fraud threat. Also, police forces and regional organised crime units were not clear about their role in the intelligence-gathering process. For example, the majority of investigators we spoke with did not routinely feed information gathered during their investigations back to the bureau. This is a missed opportunity.

A national intelligence requirement?

2.42. The National Fraud Intelligence Bureau has identified eight priority areas for intelligence gathering and has provided a list of them to police forces. However, we found little awareness of this within forces or regional organised crime units. One senior officer from a regional organised crime unit told us, "From an intelligence perspective, there is nothing that has been disseminated nationally to identify what we should be doing as a region or what the national approach is."

2.43. Officers in the regional organised crime units we visited often had little understanding of the level of demand or emerging threats from fraud. In some regions, staff told us that force fraud profiles were not shared. The result is that, in the absence of regional strategies, forces and regions are often working in isolation.

2.44. We found a similar picture in forces. Because fraud was not considered to be a priority, it rarely featured on force control strategies[29] or

[29] A control strategy is a document produced by an organisation intended to enable the organisation and others (through a shared understanding of threats) to achieve a consistent response to priorities.

problem profiles[30]. Consequently, fraud does not routinely form part of force intelligence-gathering requirements.

2.45. Staff across policing stated that the limited capabilities of the Know Fraud system created an obstacle to better performance in various respects, including understanding the demand from fraud.

2.46. We also found that the use of National Fraud Intelligence Bureau products was mixed. Some forces used the force profiles to inform their own analysis of crime trends; some did not. This was also the case for the monthly victim lists. Approaches included using the list to identify and provide additional support to vulnerable victims, sharing details with partner agencies or simply passing the list to the force neighbourhood teams.

2.47. We did not find any examples of forces routinely contributing to the national intelligence picture.

Organised crime group mapping

2.48. When a police force identifies a group of individuals whom it suspects may be involved in organised crime, they should carry out a standardised 'mapping' procedure[31] that is managed on the Police National Database.[32] HMICFRS has previously reported on the importance of mapping organised crime groups.[33]

2.49. Only one of the forces that we inspected routinely identified and mapped crime groups primarily involved in fraud. Staff told us that this had enabled a more proactive approach towards the identified groups. It also encouraged officers and staff to consider options beyond simply securing a criminal justice outcome.

[30] A problem profile is intended to provide the force with greater understanding of established and emerging crime or incident series, priority locations or other identified high-risk issues. It should be based on the research and analysis of a wide range of information sources, including information from partner organisations. It should contain recommendations for making decisions and options for action.

[31] Organised crime group mapping is used by forces, regional organised crime units, the National Crime Agency and a number of non-police organisations such as Border Force.

[32] The Police National Database is a national IT system that allows the police service to share access to and search local force information on a national basis; it is designed to provide forces with immediate access to up-to-date information drawn from local crime, custody, intelligence, child abuse and domestic abuse systems.

[33] *PEEL: Police effectiveness 2016: A national overview*, HMIC, 2017, page 100.

How is good practice and 'what works' highlighted?

2.50. Alongside the effective sharing of intelligence, we hoped to find a clear process for the evaluation and dissemination of fraud-related good practice across law enforcement, partner organisations and academia. In our view, this would encourage a national approach and assist in the early adoption of tactics that protect individuals and business from fraud.

2.51. Locally, we found little evidence of forces reviewing the effectiveness of initiatives. When reviews took place, they were very limited in nature. Nationally, senior officers told us that there "was not a defined process" for the dissemination of good practice or of tactics that were shown to be effective.

2.52. City of London Police does undertake some activity to encourage the adoption of effective practices and techniques by forces. However, this function is not explicitly identified within the agreement between the force and the Home Office, and best practice is not spread in a structured way. We believe this should be a main role for the national lead force.

The role of City of London Police in sharing best practice advice

2.53. City of London Police is responsible for a number of initiatives that are designed to assist in the sharing of best practice advice. These are as follows.

- **Peer reviews** – the force provides advice and guidance to other forces in the form of peer reviews of force structures and processes. It gives advice on 'managing and servicing fraud demand'.[34] In addition, the peer reviews also cover individual investigations, with the force offering advice and, if appropriate, support.

- **Economic Crime Academy** – established in 2012, the Economic Crime Academy operates on a self-funding model and provides training[35] to a wide range of national and international organisations including police forces, other public sector bodies, companies and individuals. Courses provided by the academy cover the full spectrum of economic crime, including fraud.

- **National user groups** – the force hosts or takes part in several policing forums that it uses to highlight best practice.

- **The fraud investigation model** – developed by City of London Police in 2014, this (see Figure 2 below) is featured in the College of Policing's

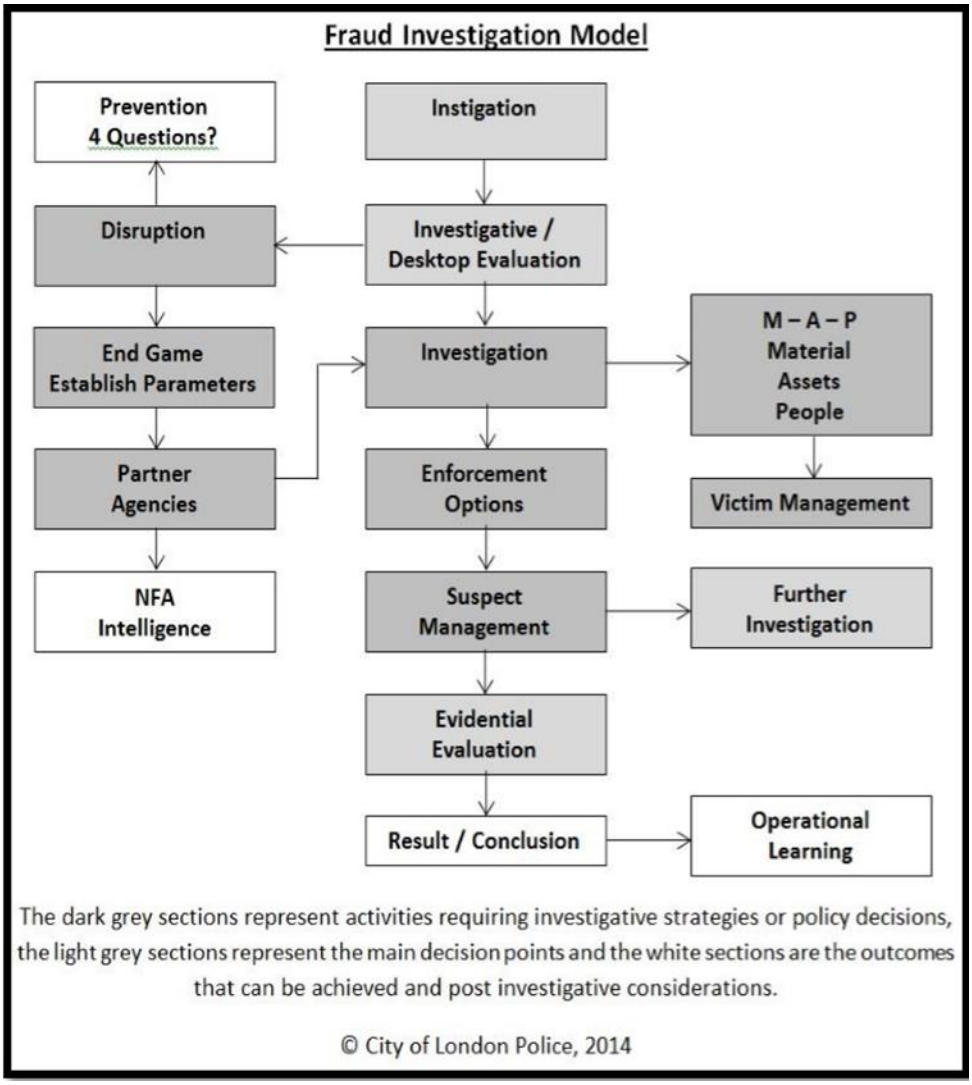
[34] *Economic Crime Annual Review 2016/17*, City of London Police, page 4

[35] *Economic Crime Academy Prospectus*, City of London Police

authorised professional practice for fraud.[36] In this document, the model is described in the following terms:

"[it] provides an alternative outcome-based framework for approaching a fraud investigation. It encourages the investigator to consider alternative outcomes and sanctions from the outset. At the same time, if a criminal investigation is to be pursued, investigators will be able to build a case that provides the greatest chance of success reflecting the seriousness of the offences under investigation."

Figure 2: Fraud investigation model



2.54. We welcome these initiatives. However, they fall short of a structured, methodical and coordinated approach to identifying, evaluating and then sharing 'what works' with forces and regional organised crime units.

[36] Authorised professional practice is authorised by the College of Policing as the official source of professional practice on policing.

2.55. The academy trains about 130 specialist fraud investigators from a variety of police forces or law enforcement agencies each year, including some overseas officers. While most forces we inspected sent officers to the academy, a small number provided their own ‘in-house’ training instead. It is therefore not realistic to view the academy as an effective means of sharing best practice advice with a wide audience.

2.56. Other organisations also have a role to play in highlighting best practice. For instance, the College of Policing is responsible for developing and publishing authorised professional practice, and hosts the Police Online Knowledge Area (POLKA) through which innovation and good practice could be disseminated. City of London Police could make more use of POLKA.

Recommendation 6

With immediate effect, the National Police Chiefs’ Council Coordinator for Economic Crime, working with the College of Policing, should take responsibility for identifying, evaluating and disseminating best practice advice on the police response to fraud.

3. Structure: How well do current structures help law enforcement to tackle fraud?

3.1. The scale of fraud, and its national and international reach, both challenge the local policing model. Local and regional structures are inadequate and dedicated fraud resources are, at best, limited in number. We found evidence of duplication and inefficient practices. Policing has several partnerships in place at the national level, but the picture at local and regional levels is more mixed. Many local and regional partnerships are ad hoc and based on individual relationships rather than a strategic approach.

3.2. Ultimately, we concluded that there is an inadequate understanding of fraud-related roles and responsibilities across police forces, regional organised crime units and national bodies. Consequently, some worthwhile activities are duplicated unnecessarily while others are not carried out at all.

How well do police forces understand the demand from fraud?

3.3. We asked the 11 forces that we inspected to provide some basic data. The data included the number of disseminations for enforcement received from the National Fraud Intelligence Bureau, the percentage of these disseminations allocated for investigation, and the total number of frauds recorded in force (i.e., all frauds, regardless of whether they were directly reported to the force or from the bureau):

- some forces were not able to provide this information;
- four forces could not provide the total number of frauds recorded;
- five forces could not tell us how many fraud crime reports had been allocated for investigation;
- seven forces could not tell us how many reports of fraud they received directly had resulted in attendance or other police activity; and
- in all 11 forces' data, there were discrepancies between the number of disseminations that the National Fraud Intelligence Bureau stated that they had sent to the force and the number the force had recorded.

3.4. We found that as fraud was not generally prioritised, the availability of analytical support was adversely affected. As one head analyst told us: "Everything is against fraud. It is not a priority, not sexy, people don't report it and it is difficult to prove, which takes time, resources and money."

3.5. One of the forces we inspected lists in its strategic assessment the number of crimes of various types. The number of frauds was listed as zero. The force had simply not considered the data held in its own records, or the data provided by the National Fraud Intelligence Bureau.

3.6. Beyond fraud not being a priority, there are several reasons for this inadequate understanding at force level. For instance, frauds are not recorded by police forces – they are recorded by the National Fraud Intelligence Bureau.

3.7. At the time of this inspection, fraud reports were disseminated by the National Fraud Intelligence Bureau to forces by email.[37] Forces are required to create local case management records for these cases.[38] Some, but not all, forces record disseminations on force crime-recording systems. In at least one force, records of disseminations were kept on a spreadsheet.

3.8. In addition to this information, police forces should also have data from calls for service that they receive directly from victims of fraud. In general terms, a call for service is a report that requires a response from the police. In the case of fraud, the Home Office Counting Rules define the circumstances that should be treated as a call for service. These are:

- "offenders are arrested by police; or
- there is a call for service to the police and the offender is committing or has recently committed at the time of the call for service; or
- there is a local suspect."[39]

3.9. Having identified a call for service, police forces should create a local record and respond to the call. They should also report the crime to Action Fraud.

[37] The new Know Fraud system allows disseminations to be notified to forces electronically on a system linked to Know Fraud.

[38] Home Office Counting Rules for Recorded Crime: Fraud, Home Office, 2018, page 2.

[39] Home Office Counting Rules for Recorded Crime: Fraud, Home Office, 2018, page 3: "'Local suspect' is where through viable investigative leads; Police can or could locate a suspect with the details provided, or have sufficient details to apprehend an offender. The word, 'local' has its everyday meaning and has been used to ensure that like any other type of crime reported directly to police, where there are local viable investigative leads police should consider the crime for investigation. This is intended to provide the same policing response as with other crime types. For example: If following an assault, a suspect can be apprehended, police could respond to that policing demand. It should be the same for fraud offences."

3.10. We expect police forces to use the information they hold from calls for service for fraud, along with information provided by the National Fraud Intelligence Bureau, to help them understand the threat and demand from fraud.

3.11. Most of the forces and regional organised crime units that we inspected did not have analysts dedicated to developing the understanding of fraud or to support specific fraud investigations. When that support was available, fraud investigations were often "at the back of the queue", to quote an interviewee.

Ineffective use of National Fraud Intelligence Bureau products

3.12. The National Fraud Intelligence Bureau sends forces monthly victim lists and six-monthly force profiles.

3.13. Some forces cross-reference the monthly lists with their own systems to identify people who need additional support. Other forces create intelligence products from the monthly lists, but these are not always put to practical use. We found one regional organised crime unit and a local force that each carried out the same analysis of the same victim list without the other knowing. More disturbingly, in one force we were told that the victim list was not used, other than to count the number of victims in the force area that month.

3.14. Forces and regional organised crime units need to improve their use of monthly victim lists in order to understand the nature of fraud in their area and determine an appropriate response.

3.15. They also need to make better use of the six-monthly fraud profiles. In all the forces and regional organised crime units that we inspected, the profiles were either used ineffectively or not at all. We found this was often because officers and staff were not aware of the National Fraud Intelligence Bureau products. This included senior officers, intelligence analysts and managers, as well as investigators and frontline officers and staff. However, some of those who were aware of them told us that the content and timeliness of these products inhibited the effective use of them by forces. This was evident in force management statements.[40]

[40] Force management statement (FMS) - annual statement, published by each force and certified by the chief constable, containing in respect of the following four years: (a) projections of demand on the force, including crime and non-crime demand, latent and patent; (b) an assessment of the state of the force's people and assets to be used to meet that demand (their condition, capacity, capability, performance, serviceability and security of supply); (c) the steps the force intends to take to improve the efficiency and economy with which the force will maintain and develop its workforce and other assets, and discharge its obligations to the public; and (d) the financial resources which the force expects to have to meet demand.

Recommendation 7

By 31 March 2020, the National Police Chiefs' Council Coordinator for Economic Crime should carry out an evaluation of two National Fraud Intelligence Bureau products: monthly victim lists and six-monthly force profiles. The evaluation should include:

- consulting with police forces to establish the uses to which these intelligence products are put; and
- identifying any opportunities to improve the products' utility or reduce the burden on the National Fraud Intelligence Bureau in compiling them.

How well do capability and capacity match identified and anticipated demand?

Capability and capacity within police forces

3.16. Capability is the ability of a police force to carry out a function. Capacity is having the resources available to carry out that function. Capability may be enabled through appropriate training of staff, the acquisition of a technical ability or other specialist resource. Capacity is obtained by ensuring that those resources, whether in the form of people or technical equipment, are available.

3.17. In the forces that we inspected, the proportion of its officers dedicated to fraud investigation varied considerably. In most cases, there was limited explanation as to why.

3.18. Four of the 11 forces we inspected had fewer than ten dedicated fraud investigators and one had only two. Two forces did not have dedicated fraud teams. Instead, fraud investigations were undertaken in an economic crime unit or financial crime team with responsibility for all economic crime including money laundering, asset recovery and fraud.

3.19. Often, we were told that fraud investigation teams had been reduced, and resources diverted to other crime priorities, to save money. It was therefore not surprising to find some fraud teams that only had capacity to deal with one investigation at a time. This meant that other fraud investigations, including complex investigations, were either not pursued at all or were allocated to officers who had not received specialist training.

3.20. We found examples of officers dealing with fraud cases who were unaware of important resources such as authorised professional practice and the fraud investigation model (see paragraph 2.53). These officers often had supervisors who were not trained to investigate fraud either. This affects the quality of investigations, the support available to staff and, ultimately, the service provided to victims.

3.21. The exceptions to this picture were City of London Police (because of its national role) and the Metropolitan Police Service (because of the high volume of disseminations it receives). Both had significant numbers of fraud investigators.

Managing demand

3.22. In some forces, additional resources had been identified to meet at least some of the demand from fraud. In one force, the police and crime commissioner used money from the Asset Recovery Incentivisation Scheme[41] to fund financial investigators, intelligence officers and victim care officers, partly to support the force's response to fraud. However, this was the exception.

3.23. The way an allegation of fraud is allocated and investigated often depends on how it is received by the force in the first place. Calls for service are generally allocated to investigating officers (and often not to specialist fraud investigators) according to local crime policies, just like any other crime reported to the police. National Fraud Intelligence Bureau disseminations are allocated according to a separate process, which is different from the way other crime is managed.

3.24. Every force we inspected had a person or team dedicated to receiving National Fraud Intelligence Bureau disseminations. Every force also had a 'triage' process to decide the appropriate action to take in each case, usually based on there being viable lines of enquiry.

3.25. Before they decide what action to take in each case, some forces review them to check whether they agree that the cases should have been allocated to them. In one force, we found that these reviews were conducted by a team of

[41] The Proceeds of Crime Act 2002 includes provisions for the confiscation of proceeds of crime after conviction in criminal proceedings, as well as a range of forfeiture, recovery and taxation powers in civil proceedings. Assets recovered are distributed to the police and other bodies to incentivise them to maximise their use of the legislation.

eight staff and took up to two months. If a force disagrees with its allocation, it can apply the 'Transcrime'[42] procedure and seek reallocation to another force.

3.26. We understand that there are a high proportion of Transcrime requests made by forces, both upon initial receipt and following further enquiries by forces. Having to check and challenge dissemination decisions is inefficient and the National Fraud Intelligence Bureau should work with forces so that cases are disseminated correctly. That said, we have concerns about the way some forces are reviewing the dissemination decisions of the bureau.

3.27. Some of the forces we inspected allocated every dissemination to fraud investigation supervisors to review the case and allocate it for investigation. Other forces used separate triage teams to decide the action to be taken in each case. These teams contained a mix of investigators, some of whom had received fraud training but some who had not.

3.28. It is important to be clear that triage can be a valid activity. For example, it may not be appropriate to allocate valuable resources to the investigation of a case that has not resulted in any financial loss, or where the investigations would be disproportionately costly. However, it is important that triage is not used for the sole purpose of suppressing demand.

3.29. Across the forces that we inspected, the percentage of disseminations allocated for investigation varied widely. In four of the forces, between 90 and 100 percent of cases were allocated. However, in one force, only 10 percent of disseminations were identified as being suitable for further investigation.

3.30. In the latter force, in one month, 96 percent of disseminations were filed without further investigations. We examined some of these cases and found that the majority had a good degree of evidence and, in some cases, suspects had been identified. In each case, reasons had nonetheless been found not to allocate it for investigation. One member of staff was quite clear that their role was to "reduce demand on investigators". They told us, "If there is an excuse not to investigate it, we will use it."

3.31. Some forces have set up teams to manage the level of demand to match their capacity, rather than developing capacity to meet that demand. This is understandable, given their finite resources and the need to prioritise. But, in

[42] 'Transcrime' procedure: Any force seeking to transfer disseminated crimes under one of the five principles contained within the fraud section of the Home Office Counting Rules must do so via the National Fraud Intelligence Bureau Crime Incident Registrars. The National Fraud Intelligence Bureau Crime Incident Registrars will make the decision as to whether a force seeking to transfer a crime will keep the crime or to which force it will be transferred. In the event of the transfer being authorised, the crime reviewers will be informed who will then disseminate the crime to the new force and update their records accordingly.

some instances, decisions not to allocate cases for investigation were questionable. We return to this theme, and the implications for victims, later in this report when we look at 'How well are fraud victims kept informed about progress of their reports?'

Recommendation 8

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should issue guidance to police forces on how to:

- accurately record and report on National Fraud Intelligence Bureau 'disseminations for enforcement', to ensure consistency and clarity for fraud recording processes (the guidance should reassert the requirement in the Home Office Counting Rules for forces to provide the case number, the crime numbers, the suspect details and the outcome details for each such dissemination);
- determine their response to National Fraud Intelligence Bureau disseminations for enforcement, ensuring consistency and clarity for victims of fraud; and
- ensure that, when a force decides not to investigate, or not to continue an investigation, the victim is provided with a clear written explanation of the rationale for that decision.

Recommendation 9

By 30 September 2019, chief constables should publish their force's policy for responding to and investigating allegations of fraud (in relation to both calls for service and National Fraud Intelligence Bureau disseminations for enforcement).

Capability and capacity within regional organised crime units

3.32. Regional organised crime units provide a range of specialist policing capabilities at a regional level that help forces to tackle serious and organised crime effectively.

3.33. In 2012, fraud investigation was identified as one of 13 capabilities that each regional unit should have.[43]

3.34. Some regional units have dedicated fraud investigation teams – although in some cases these 'teams' consisted of two people and, in one region, just a

[43] *Regional Organised Crime Units – A review of capability and effectiveness*, HMIC, 2015, page 60

single investigator. Others had merged fraud investigators and financial investigators into financial crime teams, with a greater focus on confiscation and asset recovery than fraud investigation.

3.35. One regional organised crime unit had moved its fraud investigators into a regional reactive response unit to support forces. This meant it had no dedicated regional fraud investigation team and limited ability to investigate complex or serious fraud.

3.36. In some cases, police forces had more fraud capability and capacity than the regional unit that supported them. As a result, some forces stopped referring fraud investigations to the regional unit because of a perceived or actual lack of capacity. Perversely, this has led to some regional fraud teams either seeking their own work or the regional unit further reducing the size of their fraud teams.

3.37. We found few examples of fraud being identified as a priority for regional units and we did not find any examples of assessments of the capability and capacity required to deal with fraud effectively. This further undermines the effectiveness of the NPCC roles and responsibilities grid (see paragraph 2.28) and supports the concerns raised during its development.

Action Fraud and the National Fraud Intelligence Bureau

3.38. We found that staff at Action Fraud were generally trained for their role but that high staff turnover had an adverse effect. It was clear that staff wanted to do a good job. However, a limitation they raised was that they felt unaware of how the other parts of the fraud process worked.

3.39. We found that the number of staff employed was matched to the provided budget, but the budget had not increased in proportion to the increase in reported frauds. Staff told us that they were focused on quantity rather than quality and found that they did not have time to provide full explanations to callers. Notwithstanding this, the average call length had increased from 12 minutes in 2012 to 19 minutes at the time of our inspection.[44]

3.40. Although we found a high number of abandoned calls from the public (37 percent for the period April 2017 to March 2018) and an increasing call waiting time (from April 2016 to March 2018), we saw little in terms of demand management. Action Fraud was working to shift victims from telephone to online reporting and we were told that a request had been made to increase the number of call takers (we do not know the outcome of this request).

[44] Data provided by Action Fraud to 31 March 2018.

3.41. We found a similar picture at the National Fraud Intelligence Bureau. Staff were generally well trained. However, we were told that, despite the number of frauds reported to the bureau increasing by 52,309 from 2015 to March 2018[45] (a 24.5 percent increase), the funding for staff within the bureau has remained static.

3.42. The staff workload in the bureau is determined by the number of cases selected by an algorithm within the Know Fraud system and some locally managed additional searches. In essence, the system uses a matrix to score each case and those cases that score above a predesignated threshold are passed to a team of crime reviewers for a manual review. This establishes whether there are viable lines of enquiry for a criminal investigation or opportunities to take disruptive action.

3.43. However, we found that the demand on crime reviewers has led to delays – at the time of our inspection, of up to three months. As a result, the threshold for a manual review to take place has been raised.[46] This means that some cases identified by Know Fraud will no longer be reviewed. This is a further example of demand being managed according to capacity. As a result, fewer reports of fraud are being assessed and allocated to forces for investigation.

National Crime Agency

3.44. Although 'fraud and other economic crime' was featured as one of nine national threats in the *National Strategic Assessment of Serious and Organised Crime 2018*, it was not identified by the national strategic tasking and coordination group as a national priority threat.[47] Consequently, the agency does not have dedicated fraud investigation teams but will allocate resources to investigate complex frauds on a case-by-case basis. We have previously recommended regular attendance by a City of London Police representative at the meetings of the national strategic tasking and coordination group.[48]

[45] Data provided by City of London Police to 31 March 2018.

[46] The threshold score cannot be changed on Know Fraud. Therefore, the crime reviewers take no action on those cases that have been identified by Know Fraud as reaching its score but not reaching a manually determined score.

[47] *The national tasking, coordination and governance of the response to serious and organised crime: An inspection of the National Crime Agency-led arrangements*, HMICFRS, 2018, page 18

[48] *Op cit*, page 19

Are the necessary partnerships in place to tackle fraud?

3.45. Given the breadth and prevalence of fraud, partnerships between the police and other organisations are extremely important.

3.46. Encouragingly, we found examples of the police working well with industry, local government and third sector organisations, either to protect the public or to provide additional support to victims.

3.47. At the national level, there are various well-established partnerships. At the local level, however, partnerships often rely on short-term funding, with no clear indication of what would happen when funding ceased.

National partnerships

3.48. In 2016, the government established the Joint Fraud Taskforce to tackle fraud at a high level.[49] The taskforce is "a partnership between banks, law enforcement and government to deal with fraud and to focus on issues that have been considered too difficult for a single organisation to manage alone".[50]

3.49. Although it is not within our remit to inspect bodies such as the taskforce, we welcome any initiative that brings together interested parties to tackle fraud. In its report, *Online fraud*, the National Audit Office stated: "The launch of the Joint Fraud Taskforce in February 2016 was a positive step, but there is still much work to be done."[51]

3.50. In addition to the taskforce, there are other national initiatives involving private industry. The Banking Protocol is one example with figures published by UK Finance revealing that £24.7 million of fraud has been prevented and 197 arrests made in its first 12 months.[52] This is a partnership between the police and the finance industry, and is intended to provide a consistent national response to vulnerable fraud victims. Bank staff identify vulnerable victims in the process of being defrauded and the police respond immediately, preventing the fraud from occurring.

---

[49] The Joint Fraud Taskforce is made up of representatives from government, law enforcement and the banking sector. The Taskforce includes City of London Police, the National Crime Agency, Financial Fraud Action UK, the Bank of England, Cifas and Chief Executive Officers of the major banks.

[50] Joint Fraud Taskforce Management Board, HM Government

[51] *Online fraud*, National Audit Office, 2017, paragraph 23

[52] Banking protocol prevents £25m in fraud and leads to 197 arrests, Financial Fraud Action UK, 2018

Specialist units

3.51. The City of London Police's economic crime directorate houses three specialist units. Each receives funding from government or the private sector and focuses on discrete elements of economic crime.

3.52. The funding agreements require each unit to provide regular updates about their activity and the effect they have had. These units provide an example of how appropriately resourced and funded units can function in a prioritised and proactive way.

3.53. The units are:

- The Police Intellectual Property Crime Unit – the unit has the responsibility to investigate and deter serious and organised intellectual property crime in the United Kingdom. The unit is funded by the government's Intellectual Property Office.
- The Dedicated Card and Payment Crime Unit – the unit, a joint one between City of London Police and the Metropolitan Police Service, is fully sponsored by the banking industry and supported by bank investigators and case support staff whose brief is to help stamp out organised card and payment crime across the United Kingdom.
- The Insurance Fraud Enforcement Department – a specialist police unit dedicated to tackling insurance fraud, committed to addressing high-volume and organised insurance criminality. The unit is funded by the Association of British Insurers and Lloyds of London members.

Regional and force arrangements

3.54. We found more evidence of partnership working at the local level than the regional level. However, some forces and regional organised crime units had developed, or were developing, serious and organised crime strategic partnership groups. These involved working with local authorities, Trading Standards offices and voluntary organisations. The groups were intended to provide a partnership approach to specific crime threats. Fraud was included as an identified threat in some of these groups but not all.

3.55. In general, partnerships at the regional and force level were established in an ad hoc way, often relying on short-term funding that inhibited future planning. Often, they were formed through the personal relationships of motivated staff rather than the strategic direction of leaders.

3.56. Ultimately, however strong these relationships may be, they cannot be relied on to provide long-term benefits to the public. This is an unsatisfactory way in which to approach a complex matter such as fraud.

4. Protect: How well do police forces help to protect individuals and businesses from fraud?

4.1. For this part of the inspection, we considered the advice that forces provide to people and businesses to protect themselves from fraud. We also considered whether, and how, forces identify those people and businesses who may be at increased risk from fraud, and what they do to protect them from it.

4.2. We found good examples of locally led fraud prevention work and some effective collaborative ventures between the police and the private sector. The value of these activities needs to be exploited more widely and in a more structured way.

How well do police forces help people and businesses to protect themselves from fraud?

4.3. Although fraud prevention is specifically included within the *Modern Crime Prevention Strategy*, we heard only limited references to it in relation to 'protect' (see paragraph 2.10) activity.

4.4. For example, the strategy refers to a Home Office risk assessment tool[53] that helps identify people most at risk from fraud. Only one of the forces we inspected was even considering using this tool.

4.5. Most of the forces we inspected relied to some extent on Cyber Protect[54] staff to provide advice to the public on how to protect themselves from computer-enabled fraud. Unfortunately, we saw few examples of this actually happening and, when it did, it was not proactively managed.

National campaigns

4.6. There are national public campaigns that provide fraud prevention advice. 'Take Five to Stop Fraud' is often promoted by police forces as a major part of their fraud prevention advice. It is led by UK Finance and supported by the government.

[53] *Modern Crime Prevention Strategy*, Home Office, 2016, page 12

[54] Cyber Protect staff are staff provided and trained to provide 'protect' advice in relation to cyber-crime as part of the National Cyber Crime Strategy.

4.7. City of London Police, other police forces, the National Crime Agency and the government have also promoted 'Get Safe Online'. This is a national campaign run by a not-for-profit organisation providing practical advice about how people can protect themselves and their businesses against fraud, identity theft, viruses and many other problems encountered online.

4.8. The National Fraud Intelligence Bureau, through the Multi-Agency Campaigns Group, brings together other agencies to develop advice, campaigns and alerts to provide a consistent message that is distributed nationally. In general, forces and regions use the bureau products as part of their fraud protection advice.

4.9. However, the way these products are used varies. While we found good some examples of national campaigns and alerts being adapted with local perspectives, some forces simply 'share' the messages on social media. In some cases, officers – with good intent – developed their own advice about local problems without taking account of national advice or campaigns.

4.10. The National Fraud Intelligence Bureau and Action Fraud use a range of platforms to highlight their fraud protection messages, including the Action Fraud website and various social media channels.

4.11. Action Fraud also offers the free Action Fraud Alert[55] system. Members of the public who subscribe to it receive direct, verified, accurate information about scams and fraud in their area by email, recorded voice or text message. Many forces have similar alert systems and we would encourage those forces that do have them to use them for fraud alert messages.

4.12. However, we found that once advice or alerts were issued by Action Fraud there was little national coordination of what happened next; forces and regions were free to respond as they wished. Consequently, frontline officers told us that they were often unaware of national campaigns.

Protect advice at first point of contact and during investigation

4.13. In forces and regional organised crime units, we found that call handlers and investigating officers were unable to give consistent or, at times, appropriate advice to prevent fraud. We also reviewed calls from members of the public to police contact centres and found, in most cases, that fraud prevention advice was not given.

[55] The system is provided by the National Fraud Intelligence Bureau, which is run by City of London Police as a national service. The system uses the Neighbourhood Alert Platform, which is a secure, national community messaging facility used by Police, Neighbourhood and Home Watch, Crimestoppers, Fire & Rescue Services and local authorities throughout the UK.

4.14. We found examples of investigators identifying a potential trend or risk to specific groups. One example related to organised fraud targeting farmers applying for European Union grants. Officers worked with support groups and specialist media outlets to help highlight the threat. However, this case, like others we saw, was an example of investigators identifying crime trends and then developing a local campaign from scratch, rather than linking to existing national campaigns.

Focus of activity – individuals and businesses

4.15. When it exists, fraud protection activity is generally focused on individuals rather than businesses. The officers and staff we spoke to said that engaging with businesses was difficult for a variety of reasons.

4.16. However, we did find some evidence of good practice in relation to business victims of fraud. Two regional organised crime units had worked with academia to develop a better understanding of the demands of business, and tailored their activity accordingly. This included holding events at times and locations that met the needs of local businesses, such as breakfast events on local trading estates.

4.17. We welcome this approach, but we were disappointed to see that, like other good initiatives, this learning had not been made available to other forces.

People and businesses at increased risk of fraud

4.18. While providing advice to the public is an essential part of preventing fraud, the ability to focus that advice towards those people and businesses that are at increased risk can be more effective.

4.19. In general, we found that strategies focused on offence types rather than categories of people. Even when groups of people or businesses associated with trends in offence types could be identified, they were rarely targeted with advice about protecting themselves from fraud.

4.20. The six-monthly force fraud profiles and monthly victim lists (see paragraph 1.221.22) can be used to identify trends that relate to individual forces. However, some forces are not using these products to identify and protect people at increased risk (see paragraph 3.15).

Recommendation 10

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime, when issuing to police forces advice on fraud protection that is to be given to the public (including alerts and campaigns), should take responsibility for evaluating the effectiveness of how that advice is given to the public and the effectiveness of the advice.

Area for improvement

To make improvements in this area, chief constables should improve the way their force uses the National Fraud Intelligence Bureau monthly victim lists to identify and support vulnerable victims and others who require additional support.

5. Investigation: How well do police forces investigate fraud and deter potential offenders?

5.1. The principle of locally owned investigations supported by national functions is sound but its current application is not. At all levels, we found significant problems with the way fraud is currently investigated, including numerous examples of inefficient and ineffective processes.

5.2. There are unacceptably wide variations in the quality of case handling and prioritisation, unnecessary delays in the system and a lack of proactive targeting of fraudsters, with little evidence of forces trying to prevent or restrict them from committing further offences.

5.3. During this inspection, we did not identify any discernible difference in the way frauds reported by public sector organisations were investigated, compared with those reported by individuals or businesses.

How does the centralised fraud-reporting process contribute to effective investigations?

5.4. The central reporting process is, in effect, split into two halves.

5.5. One half – Action Fraud – includes a contact centre and an online reporting platform, both of which are provided by separate private sector partners.

5.6. The second half of the process is a system, previously mentioned and referred to as 'Know Fraud', run by the National Fraud Intelligence Bureau. This contains records of all data that Action Fraud sends to the bureau, along with data provided direct to the bureau by the finance industry. The system is used to assess the viability of cases for investigation.

5.7. Action Fraud and the National Fraud Intelligence Bureau, to varying degrees, fulfil the functions intended. However, there are unacceptable problems with the current arrangements.

Are there alternatives to a central reporting system?

5.8. As well as assessing the existing system, we have considered whether there are any viable alternatives to a central reporting system.

5.9. The 2006 *Fraud Review* highlighted the difficulties faced by anyone wanting to report a fraud to the authorities. There were many organisations and agencies (including the 43 police forces) to which reports could be made.[56] The review

[56] *Fraud Review*, 2006, page 65

also identified problems with exchanging intelligence and information between those organisations.

5.10. The first central reporting system (the National Fraud Reporting Centre) was set up to tackle these problems. Moving away from a central reporting system would risk re-creating the problems that existed in 2006.

5.11. The Home Affairs Select Committee considered this in 2018. In its report, *Policing for the future*, the committee concluded: "There remains a clear requirement for a national reporting and analysis centre."[57] We agree.

5.12. We have also consulted widely. Although many of the people we spoke to identified major problems with the current process, they also accepted that there are no realistic alternatives to a central reporting system.

Responsibility

5.13. When City of London Police assumed responsibility for Action Fraud in 2014, it inherited the contact centre and the reporting platform, along with existing contractual obligations. It should be noted that, in 2015, the contact centre provider went into administration and it was largely the efforts of City of London Police that kept Action Fraud running.

5.14. Given the problems with the existing process, we have nonetheless considered whether City of London Police is the most suitable organisation to oversee the central reporting process.

5.15. The options for responsibility of the centralised function are few. They are to:

- establish a new body with national responsibility for fraud, including oversight of the national reporting process; in effect this would replicate the role and responsibilities of the previous National Fraud Authority, appear to be a retrograde step and incur significant cost with little obvious benefit;
- transfer responsibility to an existing law enforcement authority – the National Crime Agency may be an obvious choice but senior leaders at the agency had no appetite for such a transfer that, as they pointed out, would also come at a substantial cost; or
- keep responsibility with City of London Police.

5.16. We concluded that Action Fraud and the National Fraud Intelligence Bureau should remain the responsibility of City of London Police. However, just as forces and the National Crime Agency are held to account for their

[57] *Policing for the future*, Home Affairs Committee, 2018, paragraph 66

effectiveness and efficiency, all parts of the central reporting process should be too. This would include inspection by HMICFRS.

Recording of information

5.17. During the inspection, we reviewed calls to Action Fraud and the records created as a result. We found that staff at the Action Fraud contact centre had accurately recorded the details of most incidents.

5.18. Inaccurate or incomplete information inhibits the ability to link crimes or identify lines of enquiry. Recognising this, calls to Action Fraud are subject to a review by supervisors to identify errors and encourage the spread of best practice.

5.19. However, online reports are not subject to any review of their quality and, at the time of the inspection, it was possible for victims to miss out important sections of the report completely. We also found examples of missing information in reports that had been completed by police forces on behalf of victims.

Delays within the National Fraud Intelligence Bureau process

5.20. Algorithms within the Know Fraud system allocate a score to each reported case, computed from a number of factors that indicate whether the case can be solved (see paragraph 3.42). Cases with scores above a threshold are forwarded for manual review[58] to assess whether there are enough viable lines of enquiry[59] for a police investigation.

5.21. The National Fraud Intelligence Bureau has 24 crime reviewers. About 7,000 reports are identified for review each month,[60] which equates to an average of 291 reports per reviewer. Some of these reports can be assessed and reviewed within 20 minutes but others need extensive enquiries that can take more than two months to complete.

[58] A 'manual review' is the process applied to reports identified by the Know Fraud system as having certain solvability factors. They are allocated to a reviewer in the National Fraud Intelligence Bureau to determine whether further action should be taken i.e., to pursue viable lines of enquiry.

[59] 'Viable lines of enquiry' are those cases assessed as being capable of investigation.

[60] The revised Know Fraud 2 system is designed to lead to more cases being identified for dissemination to forces. This will inevitably increase the demand on National Fraud Intelligence Bureau crime reviewers (and in turn forces) and on the timeliness of review prior to sending cases to forces. HMICFRS has not inspected the new system or its effect on the centralised fraud-reporting system.

5.22. Crime reviewers use the Home Office Counting Rules[61] to determine where to send each case. However, forces return some cases to the National Fraud Intelligence Bureau with a request to transfer them to a different force (see paragraph 3.25). We found examples of the bureau taking up to four weeks to respond to these requests. In many cases, victims were not told that a request to transfer the case had been made.

How well do police respond to and prioritise allegations of fraud?

5.23. The response is inconsistent, irrespective of the nature of the victim being an individual, business or public sector organisation. The definition used by forces to identify calls for service (see paragraph 3.8) in relation to fraud varies. Also, as a result of local policies, once identified, those cases are often treated differently from those referred to the force by way of a National Fraud Intelligence Bureau dissemination.

5.24. For forces, this creates the potential for unnecessary and, in some cases unrecognised, additional demand. Also, from the victims' perspective, the response (including whether their crime will be investigated at all, and by whom) varies widely from force to force.

The initial response to allegations of fraud

5.25. Despite the centralised fraud-reporting process, not all victims of fraud report their case to Action Fraud. Instead, as mentioned previously, some report the fraud to a local police force, either by telephone or online.

5.26. When receiving calls from members of the public, forces should use the Home Office Counting Rules for fraud to decide whether they need to record the fraud and respond to it as a call for service (see paragraph 3.8), or to refer the victim to Action Fraud so that the National Fraud Intelligence Bureau can determine whether the case should be investigated and, if so, by which force.

5.27. We found that forces generally identified calls for service well. However, we often saw that forces had extended the Home Office Counting Rules definition of a call for service to include vulnerability of the victim and the opportunity to recover evidence.

[61] Home Office Counting Rules for Recorded Crime: Fraud, Home Office, 2018

Vulnerable victims of fraud

5.28. Some of the forces we inspected believed that the vulnerability of the victim was included in the Home Office Counting Rules for fraud definition of a call for service. This is not the case.

5.29. This misunderstanding is attributable to conflicting advice. We found advice provided to forces by Action Fraud in a 'Frequently Asked Questions' section on the College of Policing's Police Online Knowledge Area (POLKA). The advice states that the identification of vulnerability amounts to a call for service. However, a separate *Guide for Call Handling Staff*, also provided by Action Fraud on POLKA, provides the Home Office Counting Rules definition of a call for service.

5.30. Some forces treated a report of fraud as a call for service if they identified that the victim was vulnerable. Having dealt with the victim's needs, the cases were recorded on local systems and investigations started. In many of these cases, referral to Action Fraud would have been a more appropriate course of action. Clarity for officers and staff is required.

Recovery of evidence

5.31. Securing and preserving evidence at an early stage is an essential part of a successful investigation. However, like vulnerability, the recovery of evidence is not included within the Home Office definition of a call for service.

5.32. When a crime is reported to the police and resources are allocated to that crime, the police are generally good[62] at securing the relevant evidence. In the case of frauds reported to Action Fraud, the process is different.

5.33. As Action Fraud is a contact centre, its call handlers cannot secure or preserve evidence. In general, call handlers provide advice to victims about securing and preserving evidence themselves, such as documents or computer records. This advice is repeated in the acknowledgement letter that is sent to the victim.

5.34. As with vulnerability, some forces have extended the definition of call for service to include securing and preserving evidence. We were told that this is done because evidence could otherwise be lost because of the time it takes for cases to be disseminated.

5.35. Extending the definition of a call for service increases the demand on police forces. In some forces, investigations are started for cases that would not have been disseminated by the National Fraud Intelligence Bureau. This creates an inefficient two-tier response to fraud because cases reported

[62] *PEEL: Police effectiveness 2017: A national overview*, HMICFRS, 2018, page 45

directly to those forces are more likely to be investigated than those reported to Action Fraud.

5.36. When forces start investigating fraud reports that do not amount to a call for service, the assessment, review and allocation process managed by National Fraud Intelligence Bureau is undermined.

5.37. To be clear, we do not want forces to stop providing support to vulnerable victims or to stop providing a good level of service to victims generally. However, the decisions that forces make should not be driven by a misunderstanding of the Home Office definition.

5.38. The action that a force takes should support the principles of the central reporting process. For example, it would be entirely appropriate for forces to help vulnerable victims to report their fraud to Action Fraud, rather than treating the report as a call for service. The force should also provide the victim with a clear explanation of their decisions.

Recommendation 11

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should issue guidance to police forces in relation to fraud-related calls for service as described in the Home Office Counting Rules. The advice should make clear to forces the circumstances in which they are expected to intervene, and the circumstances in which they may refer the case direct to Action Fraud. The advice should also make clear how:

- responses to reports of fraud may adequately meet the needs of the victims;
- vulnerable victims should be identified and dealt with appropriately; and
- reports of fraud should be efficiently referred to Action Fraud.

Recording of National Fraud Intelligence Bureau disseminations

5.39. When forces receive National Fraud Intelligence Bureau disseminations, the Home Office Counting Rules require them to record the case on a case management system and to notify the bureau of the case reference number. Forces are also required to notify the bureau of the outcome of the case once it has been dealt with.

5.40. Each of the 11 forces we inspected told us that they provided outcome data to the National Fraud Intelligence Bureau on a monthly basis. However, one of the forces was unable to provide a breakdown of outcomes that they had recorded.[63]

5.41. We are concerned that this double-keying of data on different systems is inefficient, but a solution to the problem has not been identified.

Home Office Circular 47/2004

5.42. In 2004, Home Office circular 47/2004 provided chief officers with priorities to be taken into account when deciding whether to accept a fraud case for investigation. The circular also provided a list of "cases where a more cautious approach might be appropriate", meaning that there may not be a need to investigate the case. The list included, for example, cases where the victim's own behaviour had contributed to the loss.

5.43. The circular has since been withdrawn but some of the forces we inspected were still using it. In one force, the triage policy was based directly on the wording of this withdrawn circular.

Number of investigations

5.44. Of the 11 forces inspected, eight were able to state how many National Fraud Intelligence Bureau disseminations for enforcement were allocated to them in the 12 months to 31 December 2017.

5.45. For the same period, only five forces were able to state how many fraud cases in total (National Fraud Intelligence Bureau disseminations and calls for service combined) were allocated for investigation. In these five forces, the percentage of calls for service and disseminations that were investigated ranged between 24 percent and 100 percent.

5.46. Two of the forces we inspected received 46 percent of all National Fraud Intelligence Bureau disseminations for enforcement in the 12 months to 31 December 2017. Between them, they filed without further investigation 37 percent of the disseminations sent to them by the bureau. This means that a considerable proportion of all cases identified by National Fraud Intelligence Bureau crime reviewers as having viable lines of enquiry were filed by these forces without any investigative action being taken.

[63] Each force inspected was asked by HMICFRS to provide recorded fraud data that they could easily retrieve from their systems. When forces found this problematic, they were not required to search for or provide it.

National Fraud Intelligence Bureau disseminations

5.47. Throughout the inspection, we were told by investigators that National Fraud Intelligence Bureau disseminations were not easily understood, of poor quality and contained inaccurate information. They also told us that the information in disseminations was often old, so they would have to repeat enquiries already completed by the bureau to get more timely information.

5.48. Some forces have developed a template form to complete when they receive a dissemination, in order to help investigators understand what the allegations are, what information is available and the lines of enquiry.

5.49. Investigators also told us that they were frustrated by their inability to access[64] the Know Fraud system to support their investigations.

5.50. We found differing views about the purpose of disseminations. The National Fraud Intelligence Bureau told us that disseminations are intelligence packages containing a collection of crime reports, information and intelligence from which forces can develop an investigation. Police forces told us that it would be better if these were evidential packages, often known as "arrest packages".

5.51. The disseminations we reviewed were intelligence packages from which forces could develop an investigation. Although each package contained relevant information, they were not easy to read or interpret. In our view, they would be particularly difficult to use for officers who were not trained to deal with fraud and who were not routinely doing so.

5.52. National Fraud Intelligence Bureau disseminations contain references to information held within Know Fraud (which may include intelligence passed from forces) and enquiries undertaken by the crime reviewer. There was little evidence of crime reviewers proactively seeking intelligence from forces in order to establish the viable lines of enquiry and decide whether to allocate the case to a force.

5.53. Investigators told us they did not routinely send information about cases to the National Fraud Intelligence Bureau. However, we did find examples of investigators asking the bureau to conduct searches relating to information arising during an investigation.

5.54. The process is inefficient. The National Fraud Intelligence Bureau should work more closely with forces and regional organised crime units so that disseminations are timely and accurate.

[64] HMICFRS was told that in the revised system forces will have direct access to Know Fraud enabling direct research and enquiries. HMICFRS has not inspected the new system.

Recommendation 12

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should redesign the National Fraud Intelligence Bureau dissemination for enforcement documentation, to make it easier for recipients to interpret and use.

How well do police forces deal with allegations of fraud?

5.55. We know that not every fraud allegation is, or can be, investigated. We also acknowledge that not every fraud is complex or complicated and needs to be investigated by a specialist fraud investigator.

5.56. When a case is disseminated from the National Fraud Intelligence Bureau to a force (or other law enforcement agency), there is no requirement for that force to investigate the case. Each force can decide, according to its own priorities, which crimes it investigates and who should investigate them.

5.57. When a force does investigate a fraud, we expect the investigation to be thorough and professional. Crimes should be investigated by people with the right skills and experience. The more complex an investigation and the more vulnerable the victim, the more advisable it is to use a specialist investigator.[65]

5.58. We found that cases of fraud managed by specialist fraud investigators were generally investigated well. They had clear aims and objectives and were subject to regular reviews by supervisors. However, this was not always the case with those frauds investigated by non-specialist fraud investigators.

Skills and experience of investigators

5.59. We found that officers and staff who had been trained to investigate fraud were aware of and used the fraud investigation model. However, in some forces, specialist fraud investigation teams did not apply the model and were consumed with protracted investigations that took several years.

5.60. The frontline response, neighbourhood officers and Criminal Investigation Department investigators that we spoke to were generally not trained to investigate fraud and were not aware of the fraud investigation model. These officers and staff had to work on a broad range of investigations and were often also providing response policing. As a result, they had limited, if any, fraud-related supervision to assist and guide them through the investigation.

[65] *PEEL: Police effectiveness 2017: A national overview*, HMICFRS, 2018, page 44

5.61. Some of the forces we inspected had made provision for specialist fraud investigators to support and guide other investigators. Examples included fraud advice clinics where specialist investigators would attend local stations to work with officers on their cases and advise supervisors on the management of cases. Other forces were less proactive, but most specialist investigators offered support when it was needed.

5.62. One aspect of fraud investigations (as in other crime investigations) in which specialist skills are important is disclosure. Some investigators told us that they had little training in relation to disclosure and were learning as they went along. In the past, designated disclosure officers had been allocated to complex investigations, but we were often told this no longer happened because of reduced staffing levels.

5.63. The demands of the disclosure requirements were particularly significant following defence disclosures that required re-assessment of evidence. Some forces had employed additional staff on a case-by-case basis to perform this function.

5.64. The regional fraud investigation cases we reviewed were generally well managed and documented, with clear aims and objectives and regular supervisory oversight and direction.

5.65. In regional units and in forces, we found examples of other agencies involved in investigations, including Her Majesty's Revenue & Customs, Trading Standards, UK Border Agency and Department of Work and Pensions investigators. When they were involved, they were able to use their powers to assist the police investigation.

Analytical support

5.66. In forces and regions, dedicated analytical work to support fraud investigations is the exception rather than the rule.

5.67. We found some examples of investigative analysts working within specialist fraud investigation teams, but this approach was not the norm. Some investigators told us that they had to request analytical support through a force 'bidding' process. This meant that their request would be considered along with other higher priority crimes and they were unlikely to get the support they needed.

Referring cases upwards – the tasking process

5.68. Most disseminations from the National Fraud Intelligence Bureau are allocated to individual police forces. However, many cases cross force boundaries, involve organised crime groups or require specialist capabilities. In these cases, regional or national support may be required.

5.69. We found little engagement between the forces we inspected and their regional organised crime units in relation to fraud investigation. Some investigators told us they were not aware of the support or guidance that the regional or national agencies could provide. Others told us that their region had limited capacity to investigate fraud (see paragraph 3.34).

5.70. City of London Police sometimes takes on particularly complex fraud investigations as the national lead force but cannot always do so. There is no formal process for requesting City of London Police to take on a fraud investigation.

5.71. We found that regional and national tasking and coordination groups were not generally used for fraud cases. This lack of engagement and effective use of the regional and national tasking process has led to forces being responsible for major cases that involve cross-border or national criminality.

5.72. During the inspection, we were told about large-scale fraud cases 'bouncing around' between agencies. This was because no single agency directed action or took responsibility for deciding what should happen.

5.73. From time to time, particularly serious, large-scale frauds, often involving organised crime groups, will come to light. When such cases are not taken on by the Serious Fraud Office, it will fall to the police (or the National Crime Agency) to investigate them, or they may decide not to. We recognise that such cases can involve difficult decisions and the long-term commitment of significant resources.

5.74. While City of London Police is the lead force for fraud, it has no 'tasking' authority but the National Crime Agency does. To minimise unnecessary delays in decision making, using its tasking powers to provide an appropriate response to the most serious or harmful cases, the National Crime Agency has an important role to play.

Recommendation 13

With immediate effect, the Director General of the National Crime Agency, in consultation with the National Police Chiefs' Council Coordinator for Economic Crime, should ensure that the tasking powers of the National Crime Agency are used effectively in the case of serious and organised fraud.

Disruption

5.75. There are a range of powers available to disrupt criminal activity and recover or freeze assets. Some of the powers are relatively new and some, such as serious crime prevention orders,[66] are much broader in scope than just fraud. That said, we did not find much evidence that these powers were being used in fraud cases.

5.76. City of London Police has a specialist disruptions team that provides support to police forces. Much of the activity of this team (and others carrying out disruptions) relies on communication service providers voluntarily assisting the police by, for example, closing down fraudulent websites. This is particularly difficult when the service provider is not based within the United Kingdom.

5.77. Some forces use 'cease and desist' letters to request that individuals or organisations stop certain behaviour. Often the letters include a threat of legal action if the behaviour continues.

5.78. While some forces have policies to cover the use of such letters, we found examples of these letters being sent to alleged fraudsters in inappropriate circumstances. In one case, we saw the use of a cease and desist letter in relation to an alleged £50,000 fraud. Given the sum involved, we believe investigation and consideration of prosecution would have been a more appropriate response.

5.79. Disruption activity in relation to organised crime groups is already the subject of national reporting. In our report, *PEEL: Police effectiveness 2017: A national overview*, we identified "an inconsistent approach to recording, measuring and assessing the value of activity aimed at tackling serious and organised crime".[67] In that inspection, police forces told us that the process of recording and reporting such activity was too bureaucratic, which discouraged them from using it.

5.80. In this inspection, we found that disruption activity in relation to fraud is not reported on and therefore best practice is not identified. This is partly because fraud is often not considered a serious organised crime (which is true of some fraud), which means that it is not included in the mapping and reporting arrangements that apply to organised crime groups.

---

[66] Serious crime prevention orders: exist to prevent further offending after conviction of serious offences (including fraud). See Serious Crime Act 2007 – Sections 1–41 and Schedules 1 and 2, as amended by the Serious Crime Act 2015 – Sections 46–50.

[67] *PEEL: Police effectiveness 2017: A national overview*, HMICFRS, 2018, page 101

5.81. The National Crime Agency is working with forces to improve the way disruption activity for serious organised crime is reported and evaluated so that best practice can be more easily shared. We believe that forces should go further: disruption of fraudsters, whether relating to serious organised crime or not, should be evaluated and best practice shared across policing. We make a recommendation in this respect (see paragraph 2.56).

How well do police forces recognise and interact with those involved with fraud?

5.82. The threat from fraud cannot be tackled by the investigation and prosecution of offenders alone. Prevention, preparation and protection are also vital.

5.83. We were therefore disappointed not to find any evidence that individual fraudsters were being profiled by forces. Nor did we find any examples of preventative or ancillary orders being used to prevent fraud offending. These are all missed opportunities.

Organised crime groups

5.84. To succeed in disrupting and investigating serious and organised crime, forces must understand the threat clearly, map organised crime groups[68] accurately and prioritise activity against them. We found evidence that organised crime groups whose primary offence is fraud are not being mapped.

5.85. Nationally (at the end of 2017), there were 4,629 active organised crime groups in the United Kingdom, of which 842 (18 percent) were involved in fraud.[69]

5.86. At the time of our inspection, regional organised crime units were developing regional organised crime threat assessment teams, which would be responsible for mapping organised crime groups.

5.87. Only 2 of the 11 forces that we inspected routinely identified and mapped organised crime groups that were involved in fraud as a primary offence type. Investigators told us that organised crime groups involved in drugs and firearms offending were more likely to be identified than those involved in fraud. We saw evidence of this in some of the crime files we reviewed, in which offenders who met the definition of an organised crime group member

[68] Organised crime group mapping is the standardised method of assessing the risks that organised crime groups present to communities and prioritising activity against them.

[69] Data provided by the National Crime Agency – National Data Unit.

were not identified as such and organised criminality was not managed or tackled.

5.88. In regional organised crime units, organised crime groups involved in fraud were more likely to be identified and mapped, although this was not always the case. We found that most of the frauds investigated by regional organised crime units were those involving organised crime groups. Regional organised crime units were also investigating some complex regional frauds carried out by individuals rather than groups.

5.89. When fraud organised crime groups were mapped, any disruption activity was generally recorded properly in national reports. However, in one case, two regional organised crime units and one force were all investigating the same organised crime group because the group had not been mapped.

5.90. National Fraud Intelligence Bureau force profiles (see paragraph 1.22) contain a section that identifies organised crime groups engaged in economic crime (among other crime types) within each force area. The bureau also indicates on disseminations where the suspects in the case could be considered for mapping by the force. We found evidence that some intelligence staff and managers were not aware of this information.

5.91. The failure to identify and map organised crime groups involved in fraud is another unexploited chance to target fraudsters. We have some concern that management of fraud organised crime groups is not as effective as it could be, particularly when they are operating across force boundaries.

Area for improvement

To make improvements in this area, chief constables should ensure that their force improves the identification and mapping of organised crime groups in which the principal criminality is fraud.

Management of offenders

5.92. As we identified in 2017, "[T]o minimise the offending behaviour of persistent criminals … forces need to … work closely with other organisations to prevent them from reoffending".[70]

5.93. We found no evidence that fraudsters were routinely identified for integrated offender management. Proactive targeting or profiling of fraudsters was rare. We also found very little activity in forces or regional organised crime units

[70] *PEEL: Police effectiveness 2017: A national overview*, HMICFRS, 2018, page 64.

that sought to prevent people from becoming involved in fraud, or to prevent fraudsters committing further offences.

5.94. We did see some evidence of 'prevent' activity (see paragraph 2.10) with students being targeted to become 'money mules',[71] and also the use of 'suspicious activity reports'[72] to identify and prevent vulnerable people from being drawn into fraud.

5.95. We asked investigators about their use of erious crime prevention orders (see paragraph 5.75) to prevent further offending after conviction for fraud. They told us that, if they obtained an order, it would be their responsibility to manage and enforce it, which would be impractical because they were already committed to other fraud investigations. They therefore did not make the application.

Area for improvement

To make improvements in this area, chief constables should:

- ensure that fraudsters are included among those considered for serious organised crime 'prevent' tactics, including by local strategic partnership boards and through integrated offender management processes; and
- increase their force's use of ancillary orders against fraudsters.

[71] Money mules are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. Money mules receive the stolen funds into their account. They are then asked to withdraw it and wire the money to a different account, often one overseas, keeping some of the money for themselves.

[72] A suspicious activity report is a piece of information alerting law enforcement agencies that certain client or customer activity is in some way suspicious and might indicate money laundering or terrorist financing. See Submitting a suspicious activity report (SAR) within the regulated sector, National Crime Agency, 2016

6. Victims: To what extent does law enforcement consistently provide a high-quality response to victims of fraud?

6.1. It can be confusing for victims to understand where and how to report fraud. Having reported a fraud, victims often receive mixed messages about what will happen next.

6.2. In general, vulnerable victims are identified and supported well. However, the support they are given is not coordinated and often relies on short-term funding. We found little evidence of agencies seeking feedback about their services.

Action Fraud

6.3. The *Fraud Review* noted that "[it] is often confusing for victims to know who to report the fraud to"[73] and recommended that a national reporting centre be established.[74] We were disappointed to find that, some 13 years later, confusion still exists.

6.4. In its 2018 report, *Overview of fraud and computer misuse statistics for England and Wales*, the Office for National Statistics reported that the main reason victims gave for not reporting fraud was a "lack of awareness of Action Fraud".[75]

6.5. In October 2018, the Home Affairs Select Committee published its *Policing for the future* report, in which it came to a stark conclusion about Action Fraud:

> "Despite efforts to improve its response to victims of fraud, Action Fraud has irretrievably lost the confidence of the public, and reasonable expectations from victims are not being met. It is sensible to have a centralised reporting facility for fraud, but this must not simply become a way to divert and fob off victims of crime. Most importantly, it must be accompanied by a proper system to investigate crimes and respond to victims, or it will become irrelevant."[76]

[73] *Fraud Review*, 2006, page 66

[74] *Op cit*, page 278

[75] Overview of fraud and computer misuse statistics for England and Wales, Office for National Statistics, 2018, section 6

[76] *Policing for the future*, Home Affairs Committee, 2018, paragraph 50

6.6. Throughout our report, we offer judgments that are broadly consistent with those made by the Office for National Statistics and the Home Affairs Select Committee. It is plainly evident that there are major shortcomings in Action Fraud and in other parts of the system too, all of which will have adversely affected public confidence.

6.7. Consequently, the following recommendation is intended to address one of the more immediate problems concerning Action Fraud.

Recommendation 14

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime should:

- carry out (and subsequently evaluate) a campaign to raise the public awareness of the existence and role of Action Fraud; and
- provide chief constables with a description of the role of Action Fraud for uploading to force websites.

How easy is it to report fraud?

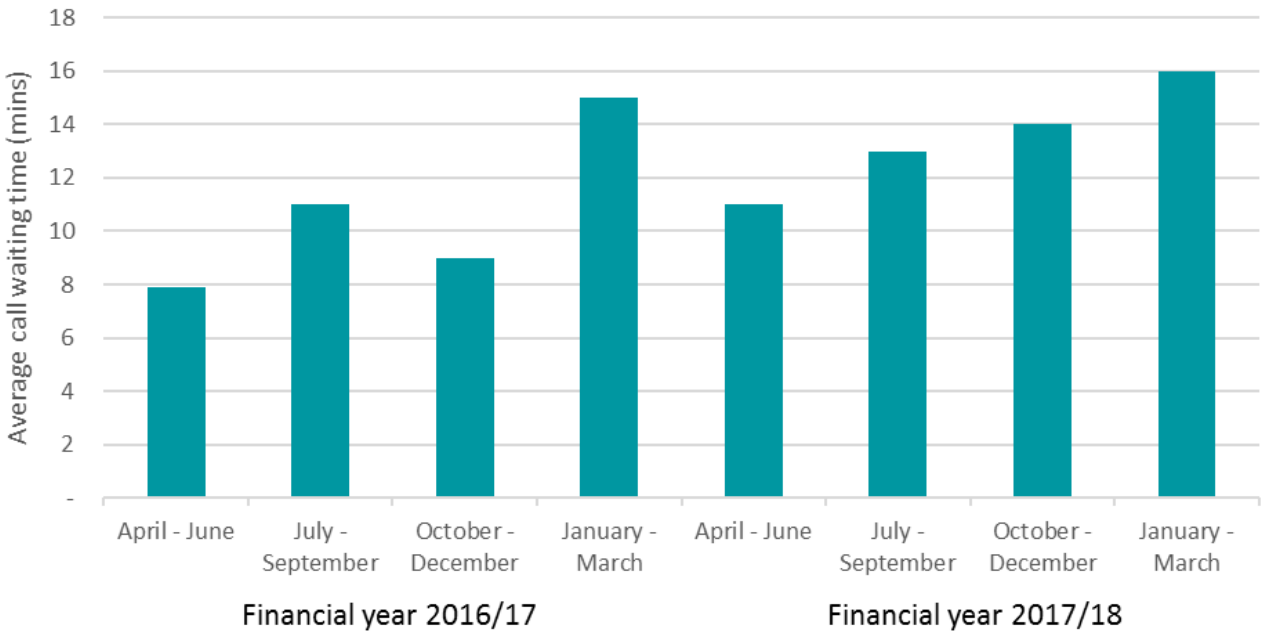
Direct to Action Fraud by telephone

6.8. Action Fraud's advisers are available by phone between 8am and 8pm Monday to Friday. Outside these hours, victims are advised to use Action Fraud's online reporting tool.

6.9. One measure of how well a call centre is performing is the proportion of calls that are abandoned by the caller before their call is answered. The average call abandonment rates for the Action Fraud contact centre between April 2017 and March 2018 was 37 percent, which was a slight increase on the previous year's figure of 34 percent.

6.10. Another measure of call centre performance is how long callers must wait before their call is answered. At the time of our inspection fieldwork, the average waiting time for the Action Fraud contact centre was 13 minutes and 40 seconds. Figure 3 shows a general increase in call waiting time over the past two years.

Figure 3: Average call waiting time (minutes) per quarter, for calls answered by Action Fraud between April 2016 and March 2018



Source: HMICFRS data collection

6.11. Although not a direct comparison, the average waiting time for Her Majesty's Revenue & Customs' helpline was just under four and a half minutes.[77] Other government departments also perform better in terms of call abandonment rates. For example, the Legal Aid Agency call centre has an average call abandonment rate of 6 percent.[78]

6.12. Lengthy waiting times and high abandonment rates are indicators of a process that is both inefficient and ineffective. We found that Action Fraud was taking little action to address these problems, other than requesting more resources and hoping that people would report fraud online, rather than by phone.

6.13. Both Her Majesty's Revenue & Customs and the Legal Aid Agency have clear targets and regularly publish details of how they perform against them. This is not the case for Action Fraud.

[77] HMRC monthly performance update: July 2018, Her Majesty's Revenue & Customs, 2018

[78] Data provided by the Cabinet Office in July 2018.

Recommendation 15

With immediate effect, the National Police Chiefs' Council Coordinator for Economic Crime should take steps to remedy the absence of published performance indicators at Action Fraud. As soon as practicable, performance indicators should be set in relation to, for example, call handling waiting times and abandonment rates, online reporting and victim satisfaction levels. Thereafter, information on performance against those indicators should be published.

Direct to Action Fraud online

6.14. As well as providing general information about fraud, the Action Fraud website includes an online tool for reporting fraud. The website is also the portal for Action Fraud's online platform for the reporting of cyber-crime.

6.15. Since this inspection concluded, the Action Fraud website and online reporting tool have been updated. Details of the revisions to the service are included in the section of this report describing the centralised reporting process (see paragraph 1.32). HMICFRS has not inspected this new functionality, but we are aware that the changes have addressed some of the problems we highlight below.

6.16. Many people who use the tool clearly find it frustrating and nearly half give up. Between April 2017 and March 2018, a total of 245,997 reports of fraud were successfully made online through the tool. Over the same period, 195,537 reports were started online but abandoned before completion. This is an abandonment rate of 44 percent.[79]

6.17. The website also provides a 'webchat facility', which is available at all times. This can be used to help complete the online form or to seek advice. Fraud cannot be reported using the webchat facility and it cannot be used to get updates about previous reports.

Reporting fraud to police forces

6.18. Despite the existence of Action Fraud, many people still report frauds to police forces. When this happens, the police will decide whether to deal with the call themselves (treat it as a call for service [see paragraph 3.8]) or advise the caller to contact Action Fraud.

6.19. In the forces inspected, we generally found that fraud victims were being advised to contact Action Fraud on the right occasions. We also found that forces were correctly identifying the cases they should respond to themselves.

[79] Data provided by Action Fraud.

However, this was not always true and we found cases that should have been treated as a call for service where victims were directed to Action Fraud.

6.20. In cases where fraud victims did not wish to report to Action Fraud, we saw evidence in each force that officers and staff would make the report to Action Fraud on behalf of the victim.[80]

6.21. However, as we identified in our 2015 report, *Real lives, real crimes*, there is still a lack of knowledge among officers and staff at all ranks about the role of Action Fraud.[81] During our reviews of calls, we found that some police call handlers incorrectly told callers that Action Fraud investigated fraud on behalf of the police.

6.22. In the calls that we reviewed and listened to, when Action Fraud call handlers identified a call for service, callers were put through to the police to deal with.

Advice to victims

Advice provided by Action Fraud staff

6.23. The drive to conclude calls quickly can make it harder for staff to give callers clear information. In turn, this leaves victims confused and can result in them calling Action Fraud again for updates on their case, which call handlers cannot provide. This increases demand, creating additional pressure to conclude calls quickly.

6.24. The only way for a victim to get an update on their case once they have made a report is by emailing a small team based within the National Fraud Intelligence Bureau.

6.25. This team[82] is advertised on the Action Fraud website as the contact team for dissatisfaction rather than a team dedicated to providing updates. We were told that victims would be advised of the email address for this team if they called requesting an update. This was corroborated by this small team, who also confirmed that a large proportion of emails they receive are requests for updates. (The changes to the system now allow victims to create an

[80] Home Office Counting Rules for fraud states: "Where victims decline this facility [to report to Action Fraud] and ask police to record a fraud, then police should take full details of the fraud and pass the details to NFIB [National Fraud Intelligence Bureau]. This will usually be by inputting the report direct to Action Fraud via on-line reporting."

[81] *Real lives, real crimes: A study of digital crimes and policing*, HMIC, 2015, page 66

[82] This process has changed with the revisions to Know Fraud in October 2018 with an online update form now available on the Action Fraud website and victims also being able to create an account to track the progress of their crime. HMICFRS has not inspected this new functionality.

account with Action Fraud that enables them to track the progress of their report and receive prevention advice relevant to them. There is also now an online update request form on the Action Fraud website.)

6.26. It is important that victims have realistic expectations of the service that Action Fraud (and police forces) can provide. They must therefore be provided with clear, concise and accurate information.

6.27. In some cases, this should include details of avenues outside the criminal justice system, such as civil or private actions, that may enable them to recoup financial losses.

Advice provided on force websites

6.28. The quality of advice about how to report fraud contained on force websites varies considerably. Some websites have clear links to Action Fraud, along with an accurate explanation of what Action Fraud does. On other sites, finding the advice is difficult and the advice itself is often unclear. In some cases, the information is misleading.

6.29. For example, one force website we visited in November 2018 describes Action Fraud as being "[r]un by the National Fraud Authority and is a one-stop reporting centre which handles all reports of fraud in the UK." The force does not provide an explanation of what is meant by "handles" and the National Fraud Authority was closed in 2014.

6.30. Other examples included:

- advising all victims of fraud to report to Action Fraud, either by clicking a link to the online reporting tool or by ringing the Action Fraud contact centre number;
- using the definition of a call for service (sometimes incorrectly) to advise victims when they should contact the force or Action Fraud; and
- advising victims that, if they feel 'particularly vulnerable', they should call the force on 101.

Recommendation 15

By 30 September 2019, the National Police Chiefs' Council Coordinator for Economic Crime should provide guidance to Action Fraud and chief constables. This is to ensure that, promptly on reporting a fraud, victims are provided with explanations of:

- the role of Action Fraud;
- the process by which their fraud report will be considered for assessment or referral to the police (or other law enforcement agency) by the National Fraud Intelligence Bureau;
- how to obtain an update on the progress of their case;
- how, following referral from National Fraud Intelligence Bureau, the decision on whether and how to investigate rests with the police (or other law enforcement agency); and
- the options open to victims of fraud to seek civil redress as an alternative (in cases where criminal investigations are not carried out or do not lead to convictions).

How well are vulnerable victims identified?

6.31. In our annual all-force inspection programme,[83] we have previously identified inconsistencies in how police forces define and identify vulnerability.[84] The College of Policing and the NPCC have sought to address this in the *National Vulnerability Action Plan 2018-2021*, which seeks to support forces in their response to vulnerability.

6.32. We recognise that this area is complex. The central reporting process for fraud makes the complexity even more pronounced. For example, there is a possibility that Action Fraud and the National Fraud Intelligence Bureau, the force where a victim lives and the force allocated the case for investigation will each use a different definition of vulnerability.

[83] HMICFRS's annual all-force inspection programme is an annual assessment of police forces in England and Wales. Forces are assessed on their effectiveness, efficiency and legitimacy. They are judged as outstanding, good, requires improvement or inadequate on these categories (or pillars) based on inspection findings, analysis and Her Majesty's Inspectors' professional judgment across the year.

[84] *PEEL: Police effectiveness 2017: A national overview*, HMICFRS, 2018, page 68

6.33. It is worth noting that businesses and public sector organisations are rarely, if ever, identified as being vulnerable. This means that they are unlikely to receive additional support to protect them from becoming repeat victims. This is despite the fact the effect of fraud on small businesses is often similar to that on an individual.

6.34. Action Fraud has adopted the definition of vulnerability used by the College of Policing: "A person is vulnerable if as a result of their situation or circumstances they are unable to take care or protect themselves, or others, from harm or exploitation."[85]

6.35. Staff working in the Action Fraud call centre receive training to identify those victims who meet that criteria and they use aides-memoire to assist them.

6.36. We found that in most, but not all, cases where vulnerability was apparent, it was correctly identified and recorded by the Action Fraud call handler.

6.37. Action Fraud staff are also able to use the 999 or 101 systems to notify the relevant local force if a victim needs immediate assistance. In less urgent cases, there are options to refer cases for 'slow-time' responses.

Reporting fraud online

6.38. The nature of Action Fraud's online reporting tool makes the identification of vulnerability more difficult. Nonetheless, there are options within the reporting process that enable victims to self-declare that they feel vulnerable because:

- "they were at risk of losing money;
- they were a repeat victim; or
- were a regular target."

6.39. Victims are asked to rate 'the incident's impact on their health or finances'.[86] These fields can be left blank. These criteria are not part of the College of Policing's definition of vulnerability. (The changes to the system now enable victims to provide information to enable an assessment of whether they are likely to become a victim of fraud again in the future.)

6.40. This information is sent from Action Fraud to the National Fraud Intelligence Bureau. Because the information is transferred several times a week rather

[85] Vulnerability, College of Policing

[86] Since this inspection concluded, the Action Fraud website and online reporting tool have been updated and some of the functionality relating to self-assessment questions has been altered. Details of the revisions to the service are included in Chapter 1 of this report. HMICFRS has not inspected this new functionality.

than immediately, it is not possible for the bureau staff to identify vulnerability immediately in all cases. This means that some vulnerable victims reporting fraud online may not get the immediate support that they need. (The changes to the system mean that information is now transferred from Action Fraud to Know Fraud in live time.)

National Fraud Intelligence Bureau

6.41. Crime reviewers within the National Fraud Intelligence Bureau are primarily focused on identifying investigative leads. It is the viability of investigative leads that dictates whether a case will be disseminated to a force. However, the bureau staff also identify vulnerable victims.

6.42. Reviewers search for words such as 'suicide' or 'mental health' in all new reports to help identify vulnerability. When a vulnerable person is identified, the reviewer can fast-track the victim's details to the victim's local force to provide support.

6.43. The monthly reports that the National Fraud Intelligence Bureau sends to forces each month do not contain any of the victims' responses to vulnerability questions. However, they do include a victim's rating of 'the incident's impact on their health or finances'. Including the answers to the vulnerability questions would help forces to identify and support vulnerable victims.

Forces

6.44. All the forces that we inspected listed the identification and support of vulnerable victims (for all crime types, not just fraud) as a priority. Each force had appropriately trained call takers who were able to identify victims of fraud who met the definition of vulnerability that their force used.

6.45. We found that in most, but not all, of the cases we reviewed, the vulnerability of the caller was identified, recorded and responded to appropriately by the police force call handler.

6.46. While fraud was generally not a priority in the forces we inspected, it was often prioritised because of the victim's vulnerability so that the force could start investigations and provide support without delay.

6.47. Many forces use a risk assessment tool, such as THRIVE,[87] to help them understand the level of threat, harm and risk posed to an individual.

[87] The Threat, Harm, Risk, Investigation, Vulnerability and Engagement (THRIVE) model is used to assess the appropriate initial police response to a call for service. It allows a judgement to be made of the relative risk posed by the call and places the individual needs of the victim at the centre of that decision.

6.48. We saw examples of Management of Risk in Law Enforcement (MoRiLE)[88] being used by police forces in strategic threat assessments. We did not see evidence of it being used tactically to assist decision making related to fraud investigations, either for deciding whether to investigate or during the investigation itself.

6.49. We found few examples of forces analysing the monthly victim lists provided by the National Fraud Intelligence Bureau. Because potential vulnerability is not explicitly identified on these lists, forces that use them have to make objective judgments based solely on the amount of money involved or the age of the victim.

6.50. We found that thresholds based on age varied across forces. For example, one force considered anyone under 18 years or over 65 years of age to be vulnerable. Another force placed the threshold at over 70 years, coupled with a threshold for the amount of money taken.

6.51. We understand why these factors may be used when deploying limited resources. However, it is yet another complicating factor in victims receiving a consistent service nationally.

Identifying additional victims

6.52. Investigating officers will often identify other victims, who may be unaware or have not reported the fraud to the police or Action Fraud. Some investigators we spoke to told us that they would report cases to Action Fraud on behalf of newly identified victims, some would ask victims to make a report themselves and some would do neither.

6.53. This is important because reporting the fraud creates an opportunity to make a formal assessment of the vulnerability of the victim and the scale of the offending. If the fraud is not reported, support arrangements may be provided on an ad hoc basis but the opportunity to put more formal arrangements in place is missed.

6.54. In some forces, newly identified victims are sent a questionnaire to assess both the circumstances of the fraud and their level of vulnerability. This information is reported to Action Fraud and support is put in place for people who need it. This approach was particularly advanced in the City of London Police 'contact hub' and in those forces and regional organised crime units that used a victim strategy within their investigation.

[88] MoRiLE is a process designed to assist law enforcement agencies to use a standardised assessment to help decision makers in identifying and prioritising threat, risk and harm. Its use complements the National Intelligence Model and National Decision Model, and links threat, risk and harm assessments to organisational capacity and capability.

How well are vulnerable victims supported?

Call for service – victim support or investigation?

6.55. When a fraud is reported directly to the police and they have identified indicators of vulnerability, some forces will support the victim, some will start an investigation and some will do both.

6.56. In paragraph 5.27, we noted that some forces have extended the definition of a call for service to include the vulnerability of the victim. We fully support those forces that want to provide additional support to those who need it most but supporting the victim does not always require forces to start an investigation. Forces should be careful about creating additional demand for themselves by starting an investigation in a case that is not a call for service. Such cases should be reported to Action Fraud so that the National Fraud Intelligence Bureau can assess them.

Responding to vulnerable victims

6.57. The way that forces respond to the needs of vulnerable victims of fraud varies considerably. Some forces have established specialist victim care units; others have established specific roles to provide support for victims of fraud. Some forces refer fraud victims to local support groups or other agencies. In a few forces, we found very little action beyond the initial response and reporting of the crime.

6.58. Identifying and providing support for vulnerable victims not only fulfils a basic responsibility of police forces, it can also help reduce demand by helping people to avoid becoming repeat victims.

National Economic Crime Victim Care Unit

6.59. In 2014, City of London Police and the Metropolitan Police Service established a pilot scheme to support vulnerable victims. The scheme created the Economic Crime Victim Care Unit to "support vulnerable people who have fallen victim to fraud and cyber-crime, with the aim being to make them feel safer and reduce the possibility of them becoming a repeat victim."[89]

6.60. In 2017, the pilot was extended to include Greater Manchester Police and West Midlands Police. The National Economic Crime Victim Care Unit work on a three-level response basis.

[89] Economic Crime Victim Care Unit (ECVCU), Action Fraud

- **Level one** – Action Fraud staff make initial telephone contact with all victims living within the participating force areas. Staff provide basic fraud prevention advice and assess the needs of the victims. If, during this assessment, a need for additional support is required, then the case is raised to level two.

- **Level two** – Specialist care staff, based in City of London Police, make further contact with those victims identified as requiring additional support. The team provides bespoke support, putting victims in touch with local support services and providing focused prevention advice to prevent repeat victimisation.

- **Level three** – This is for those victims who require further support, including a personal visit. Each force engaged in the pilot have staff available to provide one-to-one support and advice.

6.61. Forces involved in the pilot have approached the staffing of the units in different ways. For example, one force plans to use volunteers to provide bespoke personal advice to victims.

6.62. At the time of our inspection, the specialist team based in City of London Police had a three-month backlog of cases. While this is a long delay after the initial report by the victim, staff gave us examples of victims being nonetheless pleased with the contact because they had not had any other contact since reporting their fraud.

Operation Signature

6.63. Operation Signature was developed by Sussex Police as a means of providing additional support to victims of fraud. The operation is designed to prevent the most vulnerable from becoming subject to repeat targeting.

6.64. The initiative has since been adopted by several forces across the country, sometimes in different guises, but generally following the same principles.

6.65. Operation Signature focuses on vulnerable members of the community as follows:

- The early identification of potential vulnerability is important to the objective of preventing repeat victimisation.

- This is achieved by recognising vulnerability factors such as mental health or learning disabilities. However, in most cases, age is used as the determining factor.

- If a victim is identified as potentially vulnerable, a personal visit will be made to conduct a further assessment of their needs.
- Those with a high level of vulnerability will then be given support by a specialist team with links to local services or charitable partners.

Evaluation of support initiatives

6.66. We welcome the National Economic Crime Victim Care Unit and Operation Signature as good examples of law enforcement agencies attempting to identify and respond to vulnerability. Both schemes have been recognised as 'best practice models' by the NPCC.[90] However, we are aware that – at the time of the inspection – both schemes had not been formally evaluated.

6.67. Some forces argue that the focus on other priorities means that they do not have the resources to put effective responses in place. An independent evaluation of victim-focused schemes might provide evidence that would help forces and local policing bodies to determine whether redirecting resources into such schemes is appropriate.

6.68. We understand that the Home Office intends to evaluate the National Economic Crime Victim Care Unit. Given that one model may not be appropriate, or sustainable, for all forces, the Home Office may wish to extend their evaluation to include other victim-focused schemes, such as Operation Signature. It could also include those forces that have worked with charitable organisations to provide victim support.

Demand placed on third sector groups

6.69. The effective use of the National Economic Crime Victim Care Unit or initiatives such as Operation Signature may well reduce the demand on police resources. However, it may increase demand for the services of third sector organisations. Some support organisations told us that increasing demand on them will affect the quality of service they can provide.

6.70. We were therefore pleased to see examples of close working between police and crime commissioners and third sector services to deliver support to victims.

6.71. For example, one police and crime commissioner has provided additional funding to the local Victim Support scheme for two fraud case support workers. The workers contact all medium- and high-risk referrals from the police and offer advice and support. The commissioner's office also provided

[90] *The Police Service's response to vulnerable victims of fraud*, National Police Chiefs' Council, 2017, paragraph 4.2

funds to purchase call blockers[91] to provide a practical response to fraud victims' vulnerability.

6.72. As promising as these examples are, they are often based on short-term funding arrangements, including funds from sources that cannot be guaranteed, such as the Asset Recovery Incentivisation Scheme.

How well is fraud victim satisfaction assessed and managed?

6.73. We found very little evidence of forces seeking feedback about victim satisfaction in relation to fraud.

6.74. The Home Office requires police forces to provide data on a range of subjects.[92] Since 2016, the use of victim satisfaction surveys has been optional. As a result, some of the forces we inspected did not conduct satisfaction surveys at all. None of those that did included fraud as a specific category.[93]

6.75. Therefore, not only do some forces have little understanding of the demand placed on their resources by fraud but the situation is also compounded by a complete lack of awareness of the level of satisfaction among those who use their services.

6.76. However disappointing this may be, it is understandable. As we have identified throughout this report, police and crime commissioners and chief constables must place fraud within a hierarchy of competing demands presented by different crime types. However, it leaves forces with a very weak understanding.

Action Fraud

6.77. Action Fraud has used a customer satisfaction survey to help understand users' experience of the online reporting tool. However, we are not aware of any action being taken in response to it. There was nothing to help contact centre managers understand whether callers were happy with the service they received.

---

[91] Call blockers are devices that can be connected to telephone lines to screen and monitor calls. They can be set up to allow certain callers, block others or request callers to announce themselves before the call is accepted.

[92] The annual data requirement is a list of all requests for data made to all police forces in England and Wales under the Home Secretary's statutory powers.

[93] However, this is not universal. We are aware of one force, not subject to this inspection, that has continued to use satisfaction surveys and has included fraud within the criteria.

6.78. This gives the impression, rightly or wrongly, of an organisation that is unconcerned with the quality of service that it provides.

6.79. We have already highlighted the need for Action Fraud to establish and publish clear indicators for call waiting times and abandonment rates, in line with other government agencies and departments. Action Fraud should also take steps to understand the level of satisfaction of its service users – and publish its findings.

How well are fraud victims kept informed about progress of their reports?

6.80. The Code of Practice for Victims of Crime, more commonly referred to as the 'Victims' Code', sets out the services that should be provided to victims of crime.

6.81. The code sets out a list of entitlements which include:

- a written acknowledgement that a crime has been reported (including basic details of the offence);
- the provision of information on what to expect from the criminal justice system;
- being informed of the police investigation of the offence; and
- an explanation within five working days of any decision not to investigate a crime.[94]

6.82. The code distinguishes between individuals and businesses. Given the nature of fraud and the nature of its victims, we have included individuals and businesses in our definition of victims. We will therefore use the entitlements set out in the code as a guide to the service that all victims should be entitled to.

Contact following National Fraud Intelligence Bureau review

6.83. Delays within the central reporting process have a negative effect on the experiences of victims. We found considerable delays in some forces reviewing and processing disseminations. As a result, some victims can wait for months before being told what will happen with their case. This again increases the demand on Action Fraud because victims call for updates, which Action Fraud staff cannot provide. This can also have an adverse effect on the ability of victims to take civil action in relation to their fraud.

[94] Code of Practice for Victims of Crime, Ministry of Justice, 2015, page 19

6.84. We found situations in which victims could only have been left frustrated and, no doubt, bewildered at the process. For example, there were cases where victims had received a notification from the National Fraud Intelligence Bureau that their case had been allocated to a force for investigation, having already received a letter from the force in question stating that it did not intend to investigate the matter further.

Maintaining contact

6.85. Maintaining contact with victims is important, but it can be time-consuming for investigating officers. This is particularly true for those investigating fraud. In many fraud cases, although not all, there can be hundreds (and sometimes thousands) of victims.

6.86. We were therefore pleased to find examples of investigating officers adopting innovative approaches to inform victims about developments. These included the use of email newsletters and, in one case, identifying a volunteer to act as a single point of contact for all other victims. In another case, undertaken by a regional organised crime unit, a designated 'victim care officer' maintained contact with victims using pre-agreed passwords to reassure them that it was the police calling and not another fraud attempt.

6.87. City of London Police has developed a victim contact strategy for use in complex cases. We were pleased to hear from some forces and regional organised crime units that they were aware of the strategy and had been able to use it.

6.88. However, this approach was not used everywhere. We found one specialist fraud unit – which dealt with complex cases – that had no method for managing contact with a high number of victims. We were told that supervising officers had little notion of how their staff managed victim contact. In part, this was due to the absence of an effective case management system in the unit.

6.89. Some of the forces we inspected were still using an old version of the Victims' Code, which required forces to update victims every month. Since 2015, the code has required forces to tell victims how often they will receive updates, but these do not have to be on a monthly basis.

6.90. However regrettable it may be, there is often little progress made on fraud cases from month to month. Investigators told us that, in complying with the 28-day update requirement, they often did little more than apologise to victims that they had nothing new to tell them.

Informing victims that no further action will be taken

6.91. There are many reasons why officers might decide not to pursue a fraud investigation, including availability of resources or prioritisation. Often fraud is committed by people outside the legal jurisdiction of the United Kingdom and there may be no arrangements with that other country to progress the investigation. Albeit, we found examples of cases where those arrangements existed but no investigation took place.

6.92. However disappointing this may be for a victim, they have the right to be informed of these decisions and to have the rationale for the decision explained to them by the force in question.

6.93. Having decided not to investigate a case, most of the forces that we inspected wrote to victims advising them of their decision and the reasons behind it. They also offered support and advice on how to prevent fraud in the future.

6.94. However, we found one force that routinely informed victims of the decision, but without providing an explanation for it. Unsurprisingly, we were told that the force received several complaints regarding this.

Area for improvement

To make improvements in this area, chief constables should ensure that their force complies with the Code of Practice for Victims of Crime when investigating fraud.

Definitions and interpretations

In this report, the following words, phrases and expressions in the left-hand column have the meanings assigned to them in the right-hand column. Sometimes, the definition will be followed by a fuller explanation of the matter in question, with references to sources and other material that may be of assistance to the reader.

Action Fraud	United Kingdom's national fraud and cyber-crime reporting centre, providing a central point of contact for information about fraud and cyber-crime
authorised professional practice (APP)	official source of police policy and procedures, approved by the College of Policing to which police officers and staff are expected to have regard in carrying out their responsibilities
Chief Constables' Council	senior operational decision-making body for the National Police Chiefs' Council; brings together chief constables of police forces in the United Kingdom
Code of Practice for Victims of Crime	statutory code of practice issued by the Secretary of State for Justice under section 32 of the Domestic Violence, Crime and Victims Act 2004; establishes minimum standards on the rights, support and protection of victims of crime; its stated objective is to ensure that the criminal justice system puts victims first, making the system more responsive to them and easier for them to navigate; it also aims to ensure that victims of crime are treated well and receive appropriate support to help them cope and recover, and to protect them from becoming victims again; the code specifies the services that must be provided to victims of crime in England and Wales, and sets a minimum for the standard of those services; higher entitlements are set for victims of the most serious crime, persistently targeted victims and vulnerable or intimidated victims; the public sector bodies that are obliged to provide services to victims of crime are specified in the code and include police forces and police and crime commissioners; the Victims' Commissioner has a statutory duty to keep the code under regular review

College of Policing	professional body for policing in England and Wales established in 2012 to provide those working in policy with the skills and knowledge necessary to prevent crime, protect the public and secure public trust; has three complementary functions: knowledge (ensuring that, over time, policing practice and standards are based on knowledge rather than custom and convention), education (supporting the development of individual members, setting educational requirements and facilitating academic accreditation of members' expertise) and standards; its powers to set standards are conferred by the Police Act 1996, as amended by the Anti-social Behaviour, Crime and Policing Act 2014; examples of standards set by it include authorised professional practice and peer review
Economic Crime Academy	centre of excellence for training the wider economic crime community provided by City of London Police as the national policing lead for fraud
Europol	European Union's law enforcement agency, Europol uses analysis to support the law enforcement agencies of European Union member states to combat serious and organised crime, including fraud
force management statement (FMS)	annual statement, published by each force and certified by the chief constable, containing in respect of the following four years: (a) projections of demand on the force, including crime and non-crime demand, latent and patent; (b) an assessment of the state of the force's people and assets to be used to meet that demand (their condition, capacity, capability, performance, serviceability and security of supply); (c) the steps the force intends to take to improve the efficiency and economy with which the force will maintain and develop its workforce and other assets, and discharge its obligations to the public; and (d) the financial resources which the force expects to have to meet demand

Home Office Counting Rules (HOCR)	provide a national standard for the recording and counting of 'notifiable' offences recorded by police forces in England and Wales (known as 'recorded crime'); rules in accordance with which crime data – required to be submitted to the Home Secretary under sections 44 and 45 of the Police Act 1996 – must be collected; set down how the police service in England and Wales must record crime, how crimes must be classified according to crime type and categories, whether and when to record crime, how many crimes to record in respect of a single incident and the regime for the reclassification of crimes as no-crimes; specify all crime categories for each crime type including the main ones of homicide, violence, sexual offences, robbery, burglary, vehicle offences, theft, arson and criminal damage, drug offences, possession of weapons, public order offences, miscellaneous crimes against society and fraud
integrated offender management (IOM)	management of the most persistent and problematic offenders by police and partner agencies working together
management of risk in law enforcement (MoRiLE)	process designed to assist law enforcement agencies to use a standardised assessment to assist decision makers in identifying and prioritising threat, risk and harm; its use complements the National Intelligence Model (NIM) and National Decision Model (NDM) and links threat, risk and harm assessments to organisational capacity and capability
National Crime Agency (NCA)	non-ministerial government department established under the Crime and Courts Act 2013 as an operational crime-fighting agency with responsibility for leading national efforts to tackle serious and organised crime; its remit includes strengthening national borders, fighting fraud and cyber-crime and protecting children and young people from sexual abuse and exploitation; replaced the Serious Organised Crime Agency (SOCA)
National Fraud Intelligence Bureau (NFIB)	part of City of London Police, the National Fraud Intelligence Bureau processes the information received by Action Fraud along with information supplied by other agencies, such as Cifas and UK Finance, which is stored centrally on one system known as 'Know Fraud'

National Police Chiefs' Council (NPCC)	organisation that brings together 43 operationally independent and locally accountable chief constables and their chief officer teams to coordinate national operational policing; works closely with the College of Policing, which is responsible for developing professional standards, to develop national approaches on issues such as finance, technology and human resources; replaced the Association of Chief Police Officers on 1 April 2015
organised crime group (OCG)	criminals working together and involved in planning, co-ordinating and committing serious crime on a continuing basis
organised crime group mapping (OCGM)	standardised method of assessing the risks that OCGs present to communities and prioritising activity against them
PEEL	HMICFRS's police effectiveness, efficiency and legitimacy assessment; an annual programme of all-force inspections that reports on how well each force in England and Wales cuts crime (effectiveness), provides value for money (efficiency) and provides a service that is legitimate in the eyes of the public (legitimacy)
Police National Database (PND)	national IT system that allows the police service to share access to and search local force information on a national basis; designed to provide forces with immediate access to up-to-date information drawn from local crime, custody, intelligence, child abuse and domestic abuse systems, problem profiles research and analysis providing forces with greater understanding of established and emerging crime or incident series, priority locations or other identified high-risk issues; should be based on a range of information sources, including information from partner organisations, and should contain recommendations for making decisions and options for action
Police Online Knowledge Area (POLKA)	secure online collaboration tool for the policing community to network, ask questions, share insights, discuss ideas and, importantly, suggest new ways of working
regional organised crime unit (ROCU)	operational police unit endowed with regional jurisdiction and specialist capabilities to disrupt and dismantle organised crime units; officers and police staff normally are seconded to ROCUs from forces within the region.

serious crime prevention order (SCPO)	court order issued in accordance with the Serious Crime Act 2007 to protect the public by preventing, restricting or disrupting a person's involvement in serious crime
serious and organised crime (SOC)	serious offences (defined by the Serious and Organised Crime Act 2015) that are planned, coordinated and conducted by people working together on a continuing basis and whose motivation is often, but not always, financial gain
THRIVE	threat, harm, risk, investigation, vulnerability and engagement assessment used by call handlers to help assess the appropriate initial police response to a call for service
victims' code	Code of Practice for Victims of Crime

Annex A – Terms of reference

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) will undertake an inspection of the effectiveness and efficiency of the law enforcement response to fraud, including online fraud, by assessing whether:

- law enforcement has a well-designed strategy for tackling fraud, which is based on a comprehensive understanding of the fraud threat and its impact, takes account of evidence of what works, and is consistent with government policy;
- organisational structures provide the necessary capacity, capabilities and partnerships at force, regional, national and international levels to tackle fraud, for example by reducing opportunities for fraud to occur, by safeguarding and protecting individuals and businesses from fraud risks, and by investigating offences and managing fraud offenders; and
- the police service across England and Wales consistently provides a high-quality response to fraud, including by making it easy to report fraud and preparatory activity, by routinely assessing vulnerability and harm, and by assessing victim satisfaction.

Background information

The inspection will concentrate on fraud committed against individuals and businesses, as the responsibility for preventing and responding to fraud against public authorities generally lies with the organisation concerned rather than the police service. It will, however, extend to examination of the investigation of fraud against public authorities by police forces, regional organised crime units and the National Crime Agency.

The inspection will be conducted in accordance with HMICFRS's powers under the Police Act 1996 to inspect police forces in England and Wales (including force collaborations such as the regional organised crime units), and under the Crime and Courts Act 2013 to inspect the National Crime Agency. The inspection will also address the contribution of the College of Policing to the prevention of fraud, in accordance with the concordat between the College of Policing, HMICFRS and the Independent Police Complaints Commission (now the Independent Office for Police Conduct).

The inspection will not examine the work of the Serious Fraud Office (which is subject of inspection by HM Crown Prosecution Inspectorate), but the Director of the Serious Fraud Office has agreed to provide access to his staff so as to inform inspection of the police response to more serious and complex frauds.

Annex B – Methodology

Our inspection took place between March and July 2018. We visited 11 police forces in England and Wales, all 9 regional organised crime units, the National Crime Agency, Action Fraud, the National Fraud Intelligence Bureau and Europol. We also interviewed staff involved in implementing the new National Economic Crime Centre. We invited the local policing body for each of the 11 police forces to give us their views. A full list of the forces that were inspected is in Annex D – Forces and regional organised crime units inspected.

In each organisation, we interviewed the people responsible for the strategic and tactical response to fraud, and we held focus groups with relevant operational staff.

We also spoke to people from other relevant organisations, including the Serious Fraud Office and the College of Policing. We canvassed other police forces, which were not inspected, for opinions and examples of best practice. Finally, we spoke with charities and non-government organisations that provide advice and support to victims of fraud.

In total, we spoke with around 750 people to whom we are grateful for their contribution.

We reviewed documents such as control strategies, action plans, policies and procedures, some of which were specific to each organisation.

We listened to and reviewed telephone calls from members of the public to each of the forces we inspected and to Action Fraud. We reviewed investigations in each force and regional organised crime unit, and we reviewed the decisions made in the National Fraud Intelligence Bureau. In total, we reviewed around 250 calls and 250 investigations. More information about how we did this can be found in Annex E – About the dataAnnex D.

At our request, police forces, regional organised crime units and the National Crime Agency provided us with examples of cases that they felt demonstrated their approach to investigations and other activity in the fight against fraud.

We asked police forces, Action Fraud and the National Fraud Intelligence Bureau to provide us with a selection of fraud-related data. We have used this to understand the demand from fraud and how this is recorded and managed.

We reviewed force management statements (FMS), in which forces set out their current demand, future demand, capacity and capability.

We formed a fraud external reference group, which was invaluable to us in challenging and shaping our terms of reference, methodology and inspection findings.

Annex C – Legislation and types of fraud

Broadly, offences of fraud are deceptions committed to make a gain that is usually financial. Fraud takes many forms, but most of the 47 different fraud types can be dealt with under Section 1 of the Fraud Act 2006, which includes the following.

Fraud by false representation

This could include scams such as:

- **advance fee frauds**: often crude attempts to obtain money from large numbers of people at once; examples include letters or emails detailing large wins on the lottery or inheritance from an unknown relative requiring a small fee to release the money;
- **investment frauds**: often sophisticated and targeted offences relating to investment opportunities from traditional stocks and shares, property, precious metals, wine, art and even energy, which turn out to be non-existent;
- **retail fraud**: most commonly because of online shopping and not receiving the goods as described or not receiving any goods at all; and
- **banking fraud**: examples of this include mandate fraud where suspects send emails pretending to be from a business known to the victim and requesting that payment is made to a different fraudulent account.

Fraud by failing to disclose information

This is a specific offence often relating to professionals – for example, a solicitor failing to share vital information within the context of their work.

Fraud by abuse of position

This can be committed in several ways – for example, a person employed to care for elderly people taking advantage of their position of access to an account to remove money from a resident's account. Another example would be a conveyancing solicitor using their clients' funds inappropriately for their own financial gain.

In addition to Section 1 of the Fraud Act 2006, there are other offences of fraud that can be prosecuted under alternative legislation. These include:

- obtaining services dishonestly;[95]
- conspiracy to defraud;[96]
- dishonestly retaining a wrongful credit and false accounting;[97]
- business trading fraud;[98] and
- insolvency fraud.[99]

While fraud is normally financially motivated crime, not all financial crimes are fraud. The manufacture and use of counterfeit currency,[100] money-laundering offences[101] and corruption crimes[102] were not included in our inspection.

[95] These offences would be dealt with under the Fraud Act 2006, Section 11.

[96] These offences would be dealt with as common law offences.

[97] These offences would be dealt with under the Theft Act 1968.

[98] These offences would be dealt with under the Companies Act 2006.

[99] These offences would be dealt with under the Insolvency Act 1986.

[100] These offences would be dealt with under the Forgery and Counterfeiting Act 1981.

[101] These offences would primarily be dealt with under the Proceeds of Crime Act 2002.

[102] These offences would primarily be dealt with under the Bribery Act 2010.

Annex D – Forces and regional organised crime units inspected

Forces

City of London Police

Cleveland Police

Cumbria Constabulary

Dorset Police

Dyfed-Powys Police

Essex Police

Leicestershire Police

Metropolitan Police Service

Sussex Police

West Midlands Police

West Yorkshire Police

Regional organised crime units

Eastern Region Special Operations Unit

East Midlands Special Operations Unit

North East Regional Special Operations Unit

Regional Organised Crime Unit for the West Midlands Region

South East Regional Organised Crime Unit

South West Police Regional Organised Crime Unit

Tarian Regional Organised Crime Unit (Southern Wales)

Titan North West Regional Organised Crime Unit

Yorkshire and Humber Regional Organised Crime Unit

Annex E – About the data

The information presented in this report comes from a range of sources. It includes data published by the Home Office and Office for National Statistics, inspection fieldwork and data we collected directly from Action Fraud, the National Fraud Intelligence Bureau (NFIB) and the 11 police forces in England and Wales that we inspected.

When we collected data directly from police forces, we took reasonable steps to agree the design of the data collection with forces. We gave forces opportunity to check and validate the data they gave us to confirm the accuracy of our evidence. For example, we checked the data that forces submitted and raised queries when the information was notably different from that of other forces or inconsistent.

Review of calls to Action Fraud

We reviewed 100 calls to Action Fraud from victims reporting fraud between October and December 2017.

Review of National Fraud Intelligence Bureau decisions

We randomly selected and reviewed 101 cases that had been assessed by a crime reviewer at the National Fraud Intelligence Bureau and a decision made between October and December 2017 to take no further action.

Review of National Fraud Intelligence Bureau disseminations

We randomly selected and reviewed 50 National Fraud Intelligence Bureau disseminations for enforcement sent to forces between January and March 2018.

Review of telephone calls to police forces

We randomly selected and reviewed recordings of 20 telephone calls made between December 2017 and February 2018 to each police force inspected by victims reporting fraud.

Review of fraud crime files

We randomly selected and reviewed 20 police crime files in each force inspected that were recorded by the force between April and June 2017. We also received briefings on up to four complex fraud cases in force and regional organised crime units on fraud cases that had been investigated during 2017 and 2018.

When they could be identified, the cases reviewed were in relation to the following fraud offence types:

- Plastic card fraud – NFIB5A.
- Online bank account fraud – also NFIB5A.
- Application fraud (excluding mortgages) – NFIB5B.
- Insurance-related fraud – NFIB6A.
- Advance fee payments – NFIB1 excluding NFIB1D.
- Romance fraud/dating scams – NFIB1D.
- Financial investments – NFIB2.
- Online shopping and auctions – NFIB3A.
- Computer software service fraud – NFIB3E.
- Corporate procurement fraud – NFIB8B.
- Fraud (any type) with a suspect based outside the United Kingdom – no specific NFIB code.
- Fraud (any type) where the victim is a public sector authority.

Review of cases disseminated to forces where no further action was taken

We randomly selected and reviewed (where applicable) in each force inspected ten National Fraud Intelligence Bureau disseminations sent to forces where the force decided to take no further action.

Our reviews were designed to give us a broad overview of:

- the identification of vulnerability;
- the decision-making process in fraud cases;
- the effectiveness of investigations; and
- how fraud victims are treated.

We assessed these cases against several criteria. We supplemented our assessments with other evidence gathered because the small sample size meant that case review evidence alone was not a robust enough basis for assessing performance.